DataPower Operations Dashboard

Knowledge Center

Version v1.0.9.0

Before you use this information and the product it supports, read the information in "Notices".

Edition Number 9 (2018) This edition applies to IBM® DataPower® Operational Dashboard for Version 1, Release 0, Modification 9.

DPOD Knowledge Center v1.0.9.0

Welcome to IBM DataPower Operations Dashboard Knowledge Center!
Here you can find everything you need to know about IBM DataPower Operations Dashboard (DPOD).

Start with the Overview section to get familiar with the product and its benefits.
If you are a user of DPOD, go to the User Guide section where you will find details about everything that can be done with IBM DataPower Operations Dashboard.
If you are an administrator of DPOD, you will find very useful information in the admin guide about installing the product, configuring it and maintaining it in the Admin Guide section.

For existing users, please use the what's new to be updated with our new features.

Before you use this information and the product it supports, read the information in Notices

Need more help?

- **product documentation** - https://montier.atlassian.net/wiki
- **FixPack information:** http://www-01.ibm.com/support/docview.wss?uid=swg24042872
- **PDF Docs**: http://www-01.ibm.com/support/docview.wss?uid=swg21984708
- **Fix Central**: https://www-945.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm~WebSphere&product=ibm/WebSphere/WebSphere+DataPower+SOA+Appliances&release=All&platform=All&function=textSearch&text=Operations+Dashboard
- **Upgrade process**: http://www-01.ibm.com/support/docview.wss?uid=swg27048876

FAQ

You can ask now questions or provide feedback in the FAQ space DPOD FAQ

Found 0 search result(s).

Content search

Content tree

Notices

What's New in DPOD?

Overview

- Product Overview
- Technical Overview
- Frequently Asked Questions (FAQ)
- Known Limitations
- More information
- Glossary of Terms

User Guide

- Before You Start
- Web Console

- Admin Console
- Dashboards
- Investigate
- Explore
- Reports/Alerts

Admin Guide

- Installation and Upgrade
- Uninstall
- Management and Configuration
- DevOps Portal Setup and Security
- Appliance Maintenance
- Security
- High Availability, Resiliency or Disaster Recovery
- Troubleshoot
- Considerations for GDPR readiness

Reference

- System Parameters List
- Report publishing Web-Service
- OS Kernel settings
- Setting Up a Development VM for DPOD Installation on VMWare
- APIs Documentation
- Appliance Maintenance Status Codes
- DevOps Services Portal's User Scripts

ntegrations

- API Connect
- APM Integration
- Custom Transaction Log records

nsights

- Get request's latency and rate in time series for a service
- Get TPS in time series for a specific domain
- Get TPS in time series for a specific service
- Get TPS in time series for all domains
- Get TPS in time series for all services
- Get TPS in time series for erroneous request for a domain
- Get TPS in time series for erroneous request for a service

Quick Start Guide

Release Notes

Other Versions

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements or changes in the product(s) or the program(s) described in this publication at any time without notice.

Trademarks

IBM, the IBM logo, and DataPower are registered trademarks of the International Business Machines Corporation in the United States or other countries. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries.

Elasticsearch is a trademark of Elasticsearch BV, registered in the U.S. and in other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

The CentOS Marks are trademarks of Red Hat, Inc. (“Red Hat”).

VMware, vSphere, vCloud, vCloud Air, vCenter, and vRealize are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Other product and service names might be trademarks of IBM or other companies.

Overview

IBM DataPower Operations Dashboard (DPOD) is a powerful tool providing central self-service, profiling and troubleshooting capabilities across all your IBM DataPower Gateways. Using DPOD, you can investigate services and transactions processed by your DataPower cluster in near real time, down to the level of a single message.
DPOD also allows you to gather and report on statistics, view device health, track down security violations and much more.
As a complete solution, DPOD gives a user the ability to fully, easily and proactively troubleshoot their DataPower Gateways network.

DPOD offers the following capabilities

A Unified Console for all IBM DataPower Gateways in your network.

This console provides a complete and comprehensive perspective of your entire setup with Drill Down**,** fully queryable views for gateways, domains, services, all the way down to a single transaction's details. The console can be used by everyone involved in ensuring the health of services: System Administrators, Operators, Developers, Service Consumers, Service Providers and Security Officers.

Configurable security roles allow an administrator to create access restrictions for screens and data types. This enables the alignment of available information to the user's role in the business, and improve Service Level Agreements by offering **self-service** tools for common problems resolution.

A full payload data backlog for transactions

When enabled, this feature provides full transaction and message information across the IBM DataPower Gateways configured. This data can be used for troubleshooting during the development cycle or in production.

Near-immediate querying data

DPOD uses a fast, scalable, Big Data store, which enables near-immediate **querying of all the data** gathered from your DataPower Gateways.

Security insight views

DPOD provides full information logged for different types of events that may present real or potential security risks to your system. Events such as login failures, SSL handshakes, potential content attacks, policy violations and more are presented through DPOD's Security Dashboards.

Logical Transaction Grouping (Intrusive Feature)

DPOD has the capability to **group logical transactions** into a single view called Deprecated Extended Transactions. An administrator may configure a message traveling from one IBM DataPower Gateway to another to present as a single transaction in DPOD's console.

This feature will be deprecated in the near future and will be replaced with a non-intrusive mechanism introduced in v1.0.8.0 .

Full performance data

DPOD aggregates and displays full performance data on both front-end and back-end processing of services, providing immediate insights into the **origin of errors** or service latency.

Statistics and Analytics

DPOD calculates and displays statistics relating to your system, thus providing the user with insights into the working of Gateways, domains, services, and transactions. The data can be analyzed in terms of activity, latency, error percentages, memory usage and much more. Usage of these analytics data allows for proactive fine-tuning of your DataPower configuration, code, and service distribution.

System Overview

Using a series of dashboards, the user can access performance and other information pertaining the aggregated state of DataPower Gateways. The dashboards allow Drilling Down from a bird's eye view of total transaction activity, service latency or resource consumption into a single device or transaction's details.

Product Overview

What can DPOD do for me?

DPOD provides the following main benefits:

- **Speed up your troubleshooting** process by an order of magnitude, thus freeing your administrators, operators, and developers to focus on other tasks.
- **Proactive management of your Gateways** network. You can quickly gain insights into services that require performance tuning (whether on Gateway or at the back-end), appliances that require upgrades in the near future, etc. and use internal built-in alerts.
- Administrators experience a **noticeable reduction in support calls** from consumers, developers, operators and managers. Developers and operators will be able to gain a self-service, direct, immediate insights into the workings of consumed services, and will no longer depend on the availability of a Gateway administrator for debugging and troubleshooting.
- Managers gain a bird's-eye view of their Gateways and SOA network, supporting informed decision making and long-term planning.
- DPOD lets you troubleshoot **scenarios** that current **monitoring systems can not trace**. E.g. A failure before a transaction started and locating a failing transaction across multiple machines and log-extensive files.
- **Run maintenance task such Configuration Sync, Device backup and firmware upgrade** based on best practices scenario and across your Gateways cluster.
- **Provide internal information on execution flow, errors and latency issue for API Connect** developers and admins with a unique integration with API Connect.
- DPOD expose all **traditional services** in a **DevOps Portal** allowing users not only see and search configuration based on security role but also run such action such Service WSDL refresh.
- DPOD produces **a significant ROI shortly after deployment**.
- Additionally, DPOD **improves SLA performance** due to a quicker, seamless troubleshooting process.

Who in my company will benefit from using DPOD?

DPOD can improve efficiency across all organizational roles involved in ensuring your services function properly:

- **Service consumers and back-end providers** – Your consumers are able to access the DPOD console directly in order to investigate service availability or other problems. Service errors resulting from faulty back-end services can be easily tracked down and resolved between consumers and back-end providers directly, without requiring an intermediary.
  Service providers can easily view transactions by origin IP address, discover who their main consumers are, and obtain operational data such as service latency, throughput, etc.
- **System administrators** – DPOD provides your administrators with all the data required to quickly assess the Gateway network state in terms of health, service availability, security and performance. DPOD’s single viewing console removes the need to log into each Gateway separately.
- **Developers** – DPOD provides developers with a central view of services, transactions, message payloads and full performance data. It can therefore serve as an invaluable tool during the development cycle. By provisioning developers with (restricted) access to DPOD, you can free up your administrators' time by removing the onerous and time-costly task of supporting developers during the debugging process. When a problem occurs, DPOD's data quickly points out the culprit, without the need to dive deep into logs or Gateway integration code.
- **Managers** – DPOD provides team leaders, CTOs and higher-level managers with an instant yet detailed insight into the state of their SOA network and services, all at a single glance. Full SLA information is easily aggregated, using data from DPOD's database.
- **System operators** – Operators can easily troubleshoot production errors and other types of malfunctions via the DPOD console. They can successfully track down the origin of most problems, even without specific knowledge of Gateway administration. DPOD’s single viewing console removes the need to log into each Gateway separately.
- **Security officers** – DPOD provides security officers with forensic information for services and transactions. Security violations are viewable and searchable by relevant categories such as content validation (e.g. XML attacks), authentication, certificate and encryption, etc. Future certificate expiration can be configured to display well in advance using the Expired Certificates view.

How does DPOD work?

DPOD leverages existing Gateway capabilities to perform its data collection.

It is designed to provide an non-intrusive troubleshooting solution, and requires no change to existing Gateway integration code.

In the case payload collection is required, a manual subscription will be created in the Gateway for a limited period of time for the duration of debugging.

This table lists changes that DPOD performs on your Gateway objects that enable the data collection required for DPOD.

DATA SOURCES

DPOD collects its data from the following sources:

- Raw Gateway logs via the syslog mechanism - During initial setup, managed Gateways are configured to send syslog messages to DPOD. Those messages are then collected by DPOD’s syslog agents and stored into its Big Data store.
- Message payload via WS-M - DPOD can configure Gateways to send it full payload data via HTTP. The data is collected by DPOD's WS-M agents, and stored into a dedicated backlog. Payload data collection requires significant resources to collect and store (both by the

Gateway and by DPOD itself). To minimize possible impact on the system, WS-M data collection has to be manually enabled, and will remain active for a limited period of time only.

- Additional information via SOMA polling – DPOD uses SOMA services to periodically poll managed Gateways for additional data, such as hardware components status, I/O, memory consumption, etc.

WHAT SORT OF INFORMATION DOES DPOD PROVIDE?

DPOD provides the user with the following information:

- Raw Gateway logs – Including all information issued by Gateway processes, as well as sysouts from custom Gateway integration code.
- Device-level data - Hardware, CPU, memory, etc. as well as configuration information such as domains, services, and more.
- Service-level data - Memory consumption, configuration data, errors to success ratios, etc.
- Transaction performance and latency information - This includes front-end and back-end latency, as well as detailed memory consumption analytics for each action within a particular Gateway policy.
- Security data – Including certificate expiration, content violations, encryption errors, and more.
- Payload data - Available on an ad-hoc basis, only when enabled via WS-M.
- Configuration Data - Service configuration is collected and prepared for search and run, impact analysis. Configuration is also expose in a DevOps Portal.
- Audit logs - Including restarts time and firmware level changes over time.

Technical Overview

The following sections provide information about DPOD's architecture, components and usage scenarios

- Architecture
- Components
- Deployment Scenarios

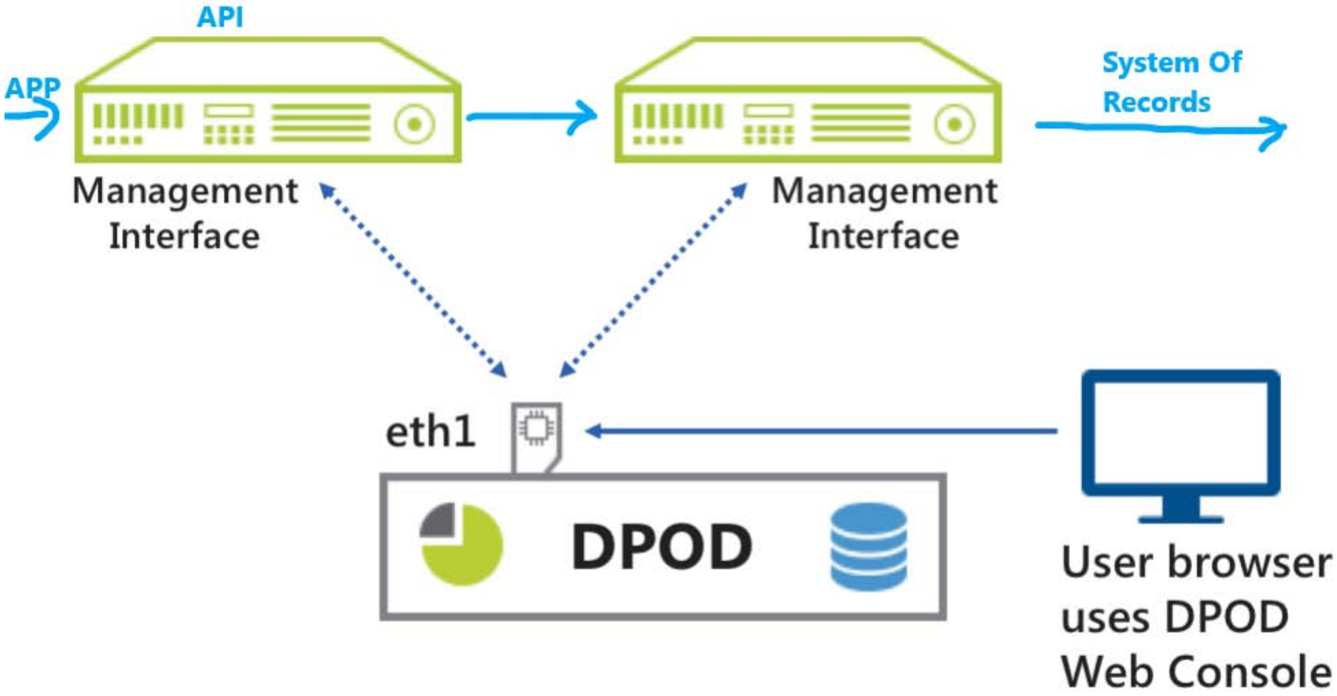
Architecture

DPOD is designed to seamlessly integrate with existing organizational DataPower architectures without requiring any changes to current DataPower deployments.

DPOD does not participate in transaction processing. Instead, it utilizes built-in DataPower capabilities such as SOMA (SOAP configuration Management), WS-Management and Log Targets to obtain the information it requires for operating.

In Order for DPOD to collect data from a monitored device (physical or virtual) it will need access to the XML Management Interface (usually via the management network interface) and the monitored device will need access to DPOD via specific TCP ports (see Firewall Requirements for details).

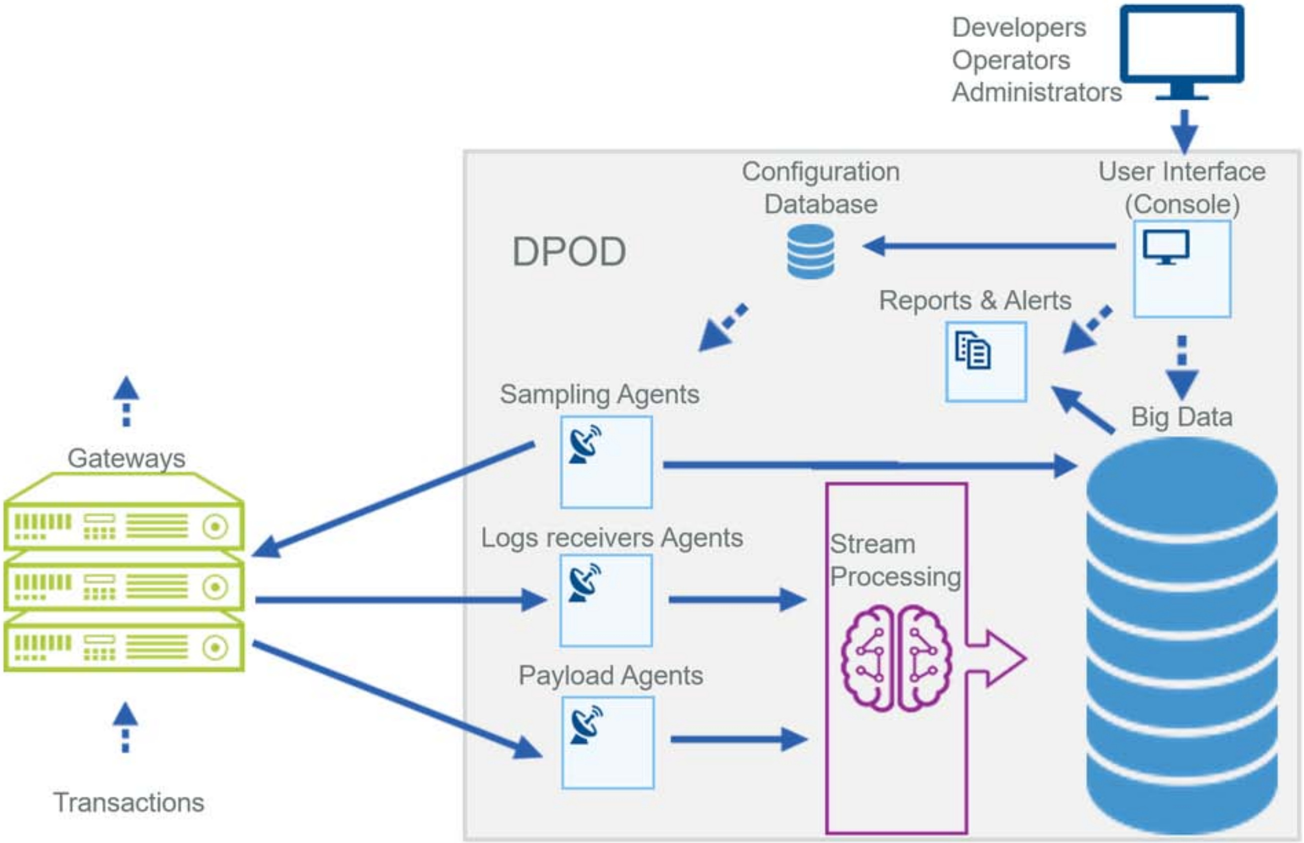
DPOD is accessible to different user types via a web interface component (Web Console). It is flexible enough to allow provisioning each user with access only to the information and functions they are authorized to use, based on RBM (Role Based Management) permissions defined by the system administrator



Components

COMPONENT DIAGRAM

The diagram below depicts DPOD's components and their interactions.



(Note: DPOD was designed for deployment using either a standalone (All in one) or distributed topology. When distributed topology is used, some of the components above will reside on different virtual/physical servers.)

BIG DATA STORE

The data flowing into DPOD through the stream processing component is stored in a Big Data store.

A new DPOD installation sets up a Big Data store that is pre-configured and optimized for DPOD's requirements. As the storage is managed automatically by DPOD’s internal components, no regular maintenance is required by users.

Configuration Database

DPOD uses an internal relational database to store its system configuration. DPOD's components read configuration properties from this database.
Configuration data is updated via the console (web interface), and is accessible by web interface and several internal components.
DPOD also stores report templates and scheduling information in this database.

LOG COLLECTION AGENTS (SYSLOG AGENTS)

The log collection agents receive Syslog log records from the monitored devices' Syslog log target, which is configured by DPOD during initial system configuration. The agents then parse the log entries, store them in the Big Data store and send them to the stream analyzing component.

DPOD automatically creates a log target on each domain (including the default domain).

Each monitored device's log target can send logs to a single log collection agent. However, a single log collection agent may subscribe to Syslog targets originating from multiple domains on a single device or several domains on different devices.

Using DPOD's user interface, a DPOD system administrator may tune the links between Syslog targets and specific log collection agent (based on the Syslog target's logging rate). Doing so helps balance the network transmissions across the system and enhances throughput and log processing on DPOD's side.

During DPOD's installation process, the installer gathers environment planning and sizing request data. Based on this information, the installer creates and configures a number of log collection agents.

SAMPLING AGENTS (DEVICE RESOURCES AND SERVICE RESOURCES)

DPOD’s sampling agents use Gateway's SOMA (SOAP configuration Management) interface for retrieving operational data for both devices (e.g. CPU, memory, load, file system and sensors) and services (e.g. service memory, service configuration). Sampling records are stored in the Big Data store.

The sampling interval used may be configured. The default sampling interval is 30 seconds for device data and 300 seconds for service data and can be changed.

WS-Management Agents (WS-M)

The DPOD WS-M agents, using the WS-Management agent on monitored devices, are responsible for processing and storing the monitored devices' service payload recording from WS-Proxy services,

Payload recording is switched off by default, and has to be enabled manually through DPOD's user interface. For security reasons, enabling the WS-M Agents in Gateway is a manual process as well. Once this is done, a subscription is registered in the WS-M agent on the monitored device.

Once a payload is recorded by a monitored device's WS-M agent from a WS-Proxy policy, the data is pushed to DPOD’s WS-M agent, which stores it in the Big Data store.

Payload recording puts the system under substantial load and therefore has to be manually enabled and its maximum duration is limited to 60 minutes.

STREAM PROCESSING

DPOD uses the Stream Processing component to stream, parse and analyze incoming data. It collects data from the log collection and WS-M agents, and operates automatically without requiring maintenance.

USER INTERFACE (WEB CONSOLE)

DPOD's user interface (Web Console) is a web-based user interface. The Console can be accessed via HTTPS and requires user/password authentication.

The console enables the user to troubleshoot, analyze and gain insights into transaction activity on monitored devices. Privileged users may also use it to update the system configuration.

REPORTS

DPOD allows users to generate various reports. These reports may be run on an ad-hoc or scheduled basis. The Reports component is responsible for processing and generating these user reports.

The system is installed with a number of built-in reports (e.g. Services Elapsed Time, System Errors and Service Memory), and privileged users are able to configure new custom reports via DPOD’s Web Console.

Reports can be saved as CSV files on the DPOD appliance file system, or sent as mail attachment via SMTP and a custom web service.

GATEWAY MAINTENANCE ACTIVITIES

A maintenance activity defines the set of maintenance actions required for a specific goal. An example of such an activity is "Perform Secure Backup on device X".
Additionally, the maintenance activity contains other specific definitions for the action. This may include for instance which certificate should be used for the Secure Backup or which deployment policy should be used for a configuration sync operation.

Current provided activities are: backup and configuration sync.

DPOD allows users to define a plan that includes a set of target gateways on which activity will be performed and a receipt on how to perform the activities.

These Activities can be integrated into an organisation wide DevOps process by REST invocation.

ALERTS

DPOD can publish alerts when certain predefined events occur, for example, when device CPU is over 80%. Alerts can be viewed and managed from the Alerts Setup page.

An alert consists of:

Alert Query - the metadata that defines the alert parameters (for example, count all the system errors occurred in the last 10 minutes in domain

DMZ). There are several built-in queries. Users customized threshold is a parameter in the query.

Alert Execution - one execution of the alert query

Alert Publishing - when an alert returns (positive) results, it will be published to interested parties via email or syslog

INTERNAL ALERTS

DPOD can send alerts on its internal services and component health status.

TRANSACTIONS EVENT FEEDER

This component handle the creation and publishing of a single aggregated logical transaction record.

One of the common usage is to push flat transactional data to external system or centralized data to have a flexible and easy access with analytics tools.

DEVOPS SERVICES PORTAL

DPOD now provides a new self-service DevOps portal for traditional services. This is a new portal dashboard where end-users can:

- Execute two new actions on SOAP Web services with **local** WSDL: validate and promote
    - The Validate action uploads your new WSDL and schema files to a temporary location, validates its compilation and creates a temporary WS-Gateway to ensure the object is up.
    - Promote action allows uploading a new WSDL and schema files to the target location (device and domain) and creating a new version of the service.
- Execute two new actions on SOAP Web services with **remote** WSDL: validate and promote
    - The Validate action updates a new or existing URL of a remote WSDL, validates its compilation, and creates a temporary WS-Gateway to ensure the object is up.
    - The Promote action updates a new or existing URL of a remote WSDL in a target location (Device and Domain), and creates a newer version of the service.

All actions require permissions set by a security policy (custom roles).

Each action may be extended or customized using Python scripts. Example scripts are open source and may be obtained from a git repository - see docs

Deployment Scenarios

DPOD is designed for deployment using either a standalone (All-in-one) or a distributed topology using remote DPOD collectors.

There are 4 basic deployment options for DPOD:

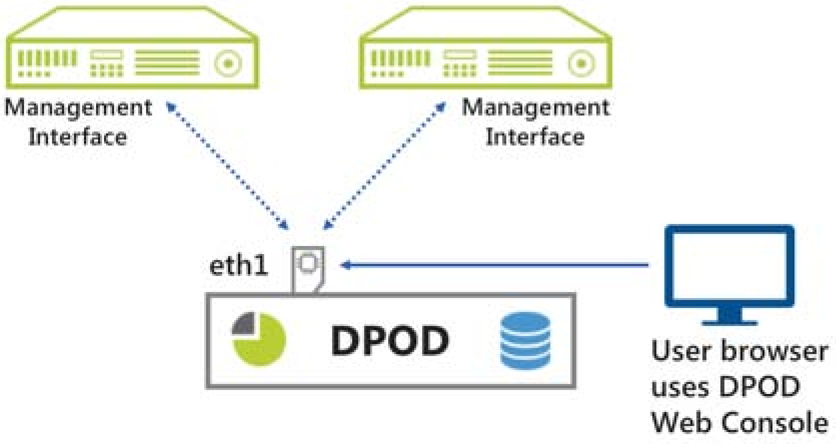
1. All-In-One with a single network interface
2. All-In-One with two network interfaces
3. All-In-One with external self-service web console
4. All-In-One with remote collector
5. High availability, resiliency and disaster recovery

SCENARIO 1: ALL-IN-ONE WITH A SINGLE NETWORK INTERFACE

This is the most common deployment scenario. All DPOD components reside on the same appliance (either virtual or physical).

A single network interface is used both for communicating with DataPower Gateway and accessing DPOD Web Console.

This scenario is appropriate for cases in which there are no organizational restrictions on providing users with direct access to DPOD's IP address.

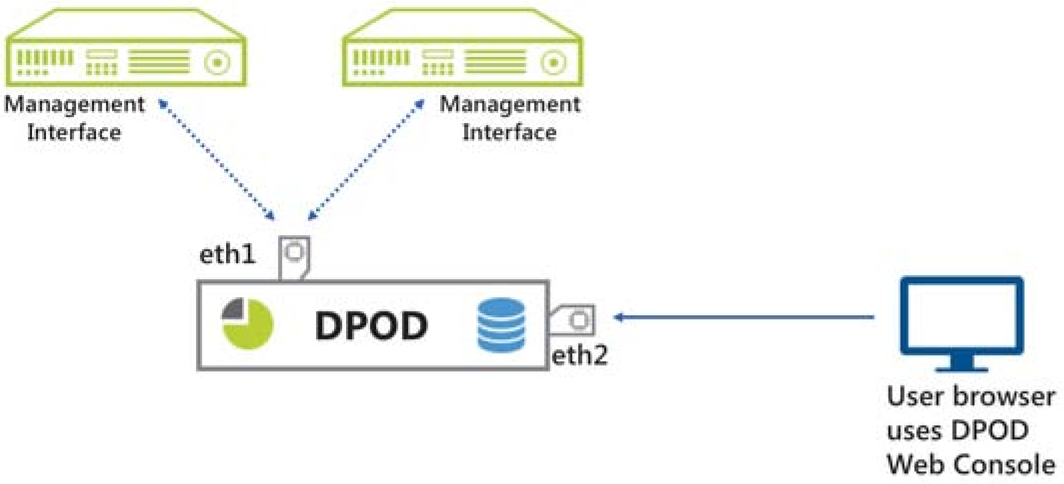


SCENARIO 2: ALL-IN-ONE WITH TWO NETWORK INTERFACES

In this deployment scenario, all DPOD components reside on the same appliance (either virtual or physical). To address network and access restrictions, DPOD uses two network interfaces:

- Network Interface 1 – for communicating with the DataPower Gateway
- Network Interface 2 – for accessing DPOD Web Console

This deployment scenario is appropriate when a separation is required between network access from Web Console users and DataPower Gateway.
Note: It is the System Administrator's responsibility to configure the second interface and make the proper static routing definitions.



SCENARIO 3: ALL-IN-ONE WITH EXTERNAL SELF SERVICE WEB CONSOLE

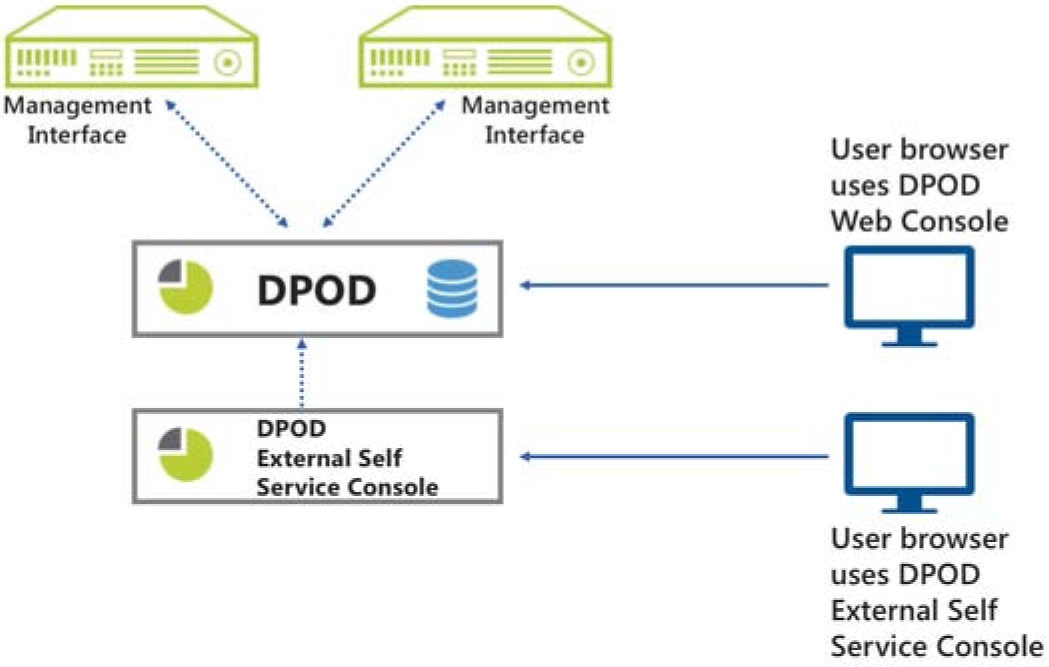
In this deployment scenario two DPOD instances are deployed. The first one is the All-In-One, **internal** instance which is fully operational. The second one is an **external** Self-Service Web Console that does not store data. It only serves as a UI component, communicating with the **internal** DPOD instance over HTTP.

This deployment scenario supports both single and dual network interfaces, as specified in the two preceding scenarios.

An organization should consider using this deployment scenario when DPOD users are members of a different network to DPOD itself, or when a separation is required between the user interface and the data stored in the system.

DPOD's External Self Service Console is an additional installation of DPOD. This second installation connects to the primary DPOD and enables developers to still use DPOD while only accessing the external DPOD, and does not require them to access through a more-secure network. This setup allows administrators to prevent unnecessary access to DataPower.

Using this deployment, developers will have access to Investigate.


Management Interface
Management Interface
User browser uses DPOD Web Console
DPOD
DPOD External Self Service Console
User browser uses DPOD External Self Service Console

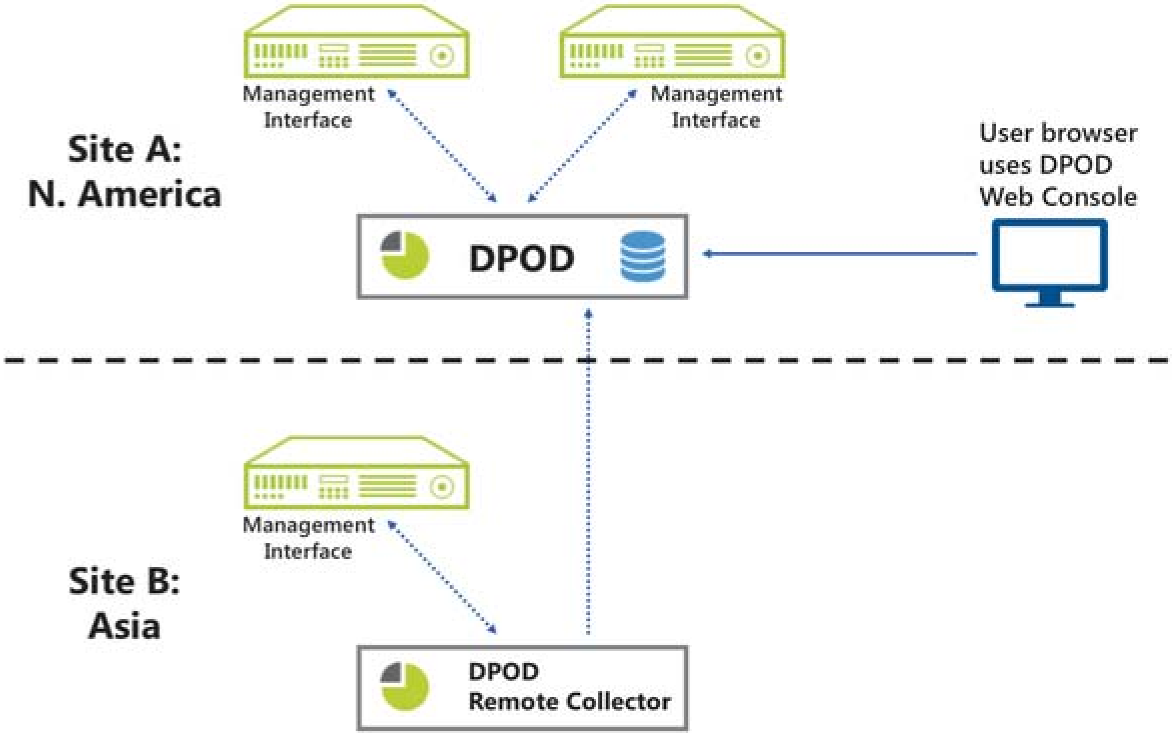
Scenario 4: All-In-One with Remote Collector

This deployment scenario addresses deploying DPOD to monitor geographically dispersed locations. Communication with these locations is performed over WAN, and are susceptible to challenges of limited or unreliable network connectivity. To address this scenario, DPOD provides the ability to deploy instances of DPOD Remote Collector alongside the All-In-One DPOD instance.

A Remote Collector is normally deployed in sites which are geographically separated from DPOD main installation site. A Remote Collector deployed in a site communicates with the DataPower Gateways there using DPOD agents. The data it collects is then sent asynchronously to DPOD main installation site.

This setup is appropriate when the existing DataPower Gateway deployment includes geographically dispersed sites, especially if network access between them is unreliable or limited (e.g. because of bandwidth).

Please see detailed instructions and requirements for the DPOD Remote Collector deployment.



SCENARIO 5: HIGH AVAILABILITY, RESILIENCY AND DISASTER RECOVERY

DPOD supports a few HA-DR scenarios. For a list of supported scenarios and detailed explanation please review the section High Availability, Resiliency or Disaster Recovery.

DPOD is not supporting Data Replication as the amount and rate of the new data to be processed is high and the resources required to support the replication are usually found as not cost effective.

DPOD HA-DR capabilities are focus on the HA of the product components without the Store collected data.

Frequently Asked Questions (FAQ)

The following pages contain frequently asked questions and their answers. The questions are grouped under the following subjects:

- General FAQ
- Technology FAQ
- Installation FAQ
- Licensing

General FAQ

In a nutshell, what is DPOD?

IBM DataPower Operations Dashboard is a powerful tool designed to increase the productivity and level of service for DataPower customers. It comprises a set of self-service tools for consumers and providers that are normally unfamiliar with DataPower and do not have access to a DataPower console.

IBM DataPower Operations Dashboard delivers first in class centralized troubleshooting capabilities alongside expert-level analysis for DataPower administrators in production and non-production environments

What sets DPOD apart from competing products?

DPOD was built primarily as a Gateway-centric tool, designed to solve real-world problems defined by DataPower experts.

DPOD uniquely combines the **transactions' perspective** - which your service consumers, service providers, operator, developers and administrators can use to resolve errors using the Self Service user interface - with an administrative perspective - which includes statistics, full resource usage information, device health, etc.

DPOD has also the following unique features for Gateway’s Gateway:

1) DPOD is that it monitors early-processing faults, such as SSL handshakes and fault URLs. This type of errors cannot be caught by error handling rules, and DPOD provides a distinct advantage in troubleshooting these errors quickly and effortlessly.

2) DPOD sample services configuration and compares them on ever time intervals.

3) DPOD provide you analytics and history on your Device/Domain restarts, shutdown and reboots.

4) DPOD provide you information on your Objects operational status for Object that are enabled.

What do your customers say is the best thing about DPOD?

All our customers say that the best thing about DPOD is that it exists! When we press them for more, they first mention how DPOD allows them to quickly and easily track down errors, and then they tell us that ever since provisioning consumers, providers, and developers with self-service access to DPOD’s Web Console, the number of support calls they are fielding has dropped significantly, allowing them to focus on their own tasks rather than mundane maintenance.

What makes DPOD the best troubleshooting tool for DataPower?

The best thing about DPOD is how quickly you can track down faulty transactions. Without it, it is nearly impossible to find a single error within Gateway’s logs, as they are swamped with a myriad of other messages that roll out too quickly.

Currently, there is no good way to store and search Gateway’s logs for messages by content, and the problem grows linearly with additional DataPower Gateways. This will require manually going into each and every one of them - an unrealistic task in most sites.

This usually means that you’ll have to re-create the error condition in real-time – a highly problematic requirement in production systems – and even this method does not guarantee you'll find the message you are looking for.

With DPOD, you can pinpoint faulty services and transactions in a heartbeat, whether it occurred a few seconds or a week ago. You can search for errors, components, services, and even run queries based on message content.

DPOD lets you view all your messages on a single screen, or you can drill down into the appliance, service or transaction details.

We have found that customers who use this unique feature of DPOD improve their troubleshooting times by an order of magnitude.

Who in my organization will benefit from using DPOD?

The short answer is: your entire staff will benefit from using DPOD.

Developers will be able to track down errors in any DataPower machine throughout the network with a click of a button.

Administrators, using DPOD’s built-in administrative reports and charts, will be able to ensure all your DataPower Gateways are running smoothly, and receive alerts on any malfunction.

Service Consumers and Service Providers can use the self-service roles-based UI to track down their specific transactions.

Architects and efficiency consultants will be able to use DPOD to obtain a complete overview of business transaction times, and quickly drill-down into the most problematic services.

Finally, using DPOD’s bird’s-eye view of the health and performance of your entire DataPower setup, your management staff will be able to make informed decisions on the future road-map of your SOA infrastructure.

What sort of ROI can I expect from using DPOD?

DPOD will enable you to track down errors extremely quickly, compared with either using DataPower by itself or using a competing monitoring product.

This translates directly into time your developers and administrators spend resolving malfunctions, in production as well as during development or unit tests time.

DPOD helps your staff to focus on what they’re supposed to do, and can significantly increase your service up-time.

In the long run, you can expect DPOD to help you manage your DataPower Gateways far more efficiently compared to other methods available.

DPOD provides you with crucial, single-view and easy to understand information on the slowest, most error-prone and resource-hungry services in your system. This allows you to focus on improving these problematic services, which will in turn improve performance and response-time for the entire appliance and reduce licensing costs.

What sort of reports can DPOD generate?

Right off the bat, DPOD offers you reports, statistics and graphs of all your transactions, services and appliances. We have configured a wide array of views and graphs into DPOD’s Console, but you can also execute, schedule and even create new reports which may be stored on DPOD's file system or emailed as spreadsheets.

Can I see a live demo?

Sure! Please contact your IBM sales representatives for details.

If you want a full guided tour of DPOD features and capabilities, send us an email, and we will schedule an online session between you and one of our team members.

Technology FAQ

Where does DPOD store its data?

DPOD stores all of its data in a Big Data store, providing blazing fast search, chart and report capabilities. It’s so fast, you’ll find that you don’t have to worry about how much data you store. A typical query on 1TB log data will return results in just under a second.

How long does DPOD store transaction and monitoring data for?

It depends on your available storage, as well as the number of appliances and services you wish to monitor. Once you allocate DPOD a specific amount of disk-space, it will optimize its usage according to the message types: business transactions will be saved the longest, for years if you have the space, and more volatile messages may be deleted after a few days. DPOD can easily handle terabytes of data, so just give it as much space as you can.

How long after the transaction occurs will I see it in DPOD?

DPOD will show you a near real-time view of transactions running through your DataPower machines. Transactions are normally viewable in DPOD's UI within seconds.

How does DataPower send monitoring data to DPOD?

DataPower sends information to DPOD via Syslog messages and SOAP messages (when enabling W-SM). DPOD also uses SOMA requests to collect sample data such as resource utilization and sensor information. You do not have to set anything up – DPOD will configure everything for you (See the topic about setting up your DataPower Gateways).

Can DPOD handle large production loads?

Yes. As long as you ensure your hardware meets the necessary requirements -DPOD will take care of the rest. We have not found a limit to DPOD’s processing capabilities yet.

How does DPOD scale?

DPOD was built to scale to infinity. Its core is made up of proven distributed cloud technologies.

DPOD can scale both horizontally - by improving existing hardware, and vertically -by adding more DPOD nodes to your network.

You can add DPOD nodes to your setup at any time, with a minimal configuration hassle.

Does DPOD require any changes to my existing code or infrastructure?

No. DPOD's data collection is mostly non-intrusive for a service level and asynchronous. It requires no significant changes to existing architecture or integration code.

The only service level intrusive feature is the optional Extended transaction feature that adds a new Transformation Action to the end of each rule of a Processing Policy. This Transformation Action injects a correlation id to the message and writes one syslog message.

There some to Objects of connected Gateways at Device /Domain level such creating log targets, create Host Alias and enable statistics.

> Please review the full list of changes that will be performed to the Gateway.

Does DPOD have a significant impact on service performance?

No. Since DPOD uses existing DataPower capabilities, a performance hit of no more than 5% is expected under normal operations. However, enabling message payload recording will likely incur significant resource consumption. Therefore, message payload recording can only be enabled for a limited time period.

Does sending logs to DPOD incur significant network overhead?

Generally, no. If only syslog logs are collected, network overhead is usually negligible. However, if message payload recording has been enabled, network overheads grow, depending on payload size and throughput.

Installation FAQ

SHOULD DPOD BE INSTALLED AS A VIRTUAL MACHINE OR ON DEDICATED HARDWARE?

It depends. DPOD can either operate as a Virtual Machine or be installed on a dedicated machine. For most installations, a VM setup will suffice. For high-loads scenarios, DPOD should be installed on a dedicated physical machine.

For additional detailed see – Hardware and Software Requirements.

WHAT SORT OF HARDWARE DO I NEED?

It depends on your monitored device setup and your monitoring needs.

We have found that a DPOD all-in-one Virtual Machine will work well with about 5 monitored device appliances, with moderate traffic - ~ 100 TPS of DataPower Transactions.

For busier systems, we recommend using a dedicated physical server – a moderate server can usually serve up to 15-20 monitored devices.

Once we get to know your requirements, we will send you exact hardware specifications, customized to your needs. You can find more information about minimum hardware requirements at Hardware and Software Requirements

DOES DPOD REQUIRE INSTALLATION?

When you purchase DPOD, you will be provided with an ISO file, either on a DVD or downloaded directly from our Releases Page. The installation itself is a simple 10-15 steps wizard. Typically, it takes about 20 minutes to set up your first DPOD node.

DOES DPOD SUPPORT MONITORED DEVICES THAT ARE DISTRIBUTED ACROSS A WIDE GEOGRAPHICAL REGION?

Yes, we have a special installation topology for geographically distributed sites. In this setup, local DPOD agents will collect data in each site, and then forward it to a central data store.

The installation is simple and only requires a few additional configuration steps

HOW DO I SET UP MY MONITORED DEVICES TO SEND DATA TO DPOD?

Setting up a monitored device to be monitored by DPOD is quick and easy. You only need to set your device’s system identifier, enable the XML Management Interface and add the appliance to DPOD with the click of a button.

The whole process takes just a couple of minutes.
See DPOD’s Installation Guide on Adding Monitored Devices

WHAT DATAPOWER FIRMWARE VERSIONS ARE SUPPORTED?

DPOD supports DataPower firmware 7.6.x+.

We know that customers are using DPOD to monitor appliances running on versions 6.x and even 5.x but on not all features are available for them.

Anyway support will only be provided to issues related with firmware 7.6.x+.

DOES DPOD SUPPORT DATAPOWER VIRTUAL APPLIANCE?

Yes. See question on supported editions and models below

WHICH DATAPOWER EDITIONS AND MODELS DOES DPOD SUPPORT?

DPOD supports IBM DataPower IDG, IDGX2 and the new IBM DataPower Gateway, both physical and virtual. B2B, Tenant and Integration module are supported.

ISAM modules will be support is on our road-map.

License Model FAQ

DPOD's Licensing is based on the number of **Application Instance (**also referred as Gateways or Monitored Device **)** connected to DPOD and managed by DPOD.

A Monitored device is any IBM DataPower Gateway whose version and edition is supported by DPOD.

The following are examples of **Application Instance**:

- One instance of IBM DataPower Gateway Virtual Edition reporting to DPOD = One Application Instance.
- One instance of IBM DataPower Gateway Virtual Non-Production Edition reporting to DPOD = One Application Instance.
- One instance of IBM DataPower Gateway Appliance reporting to DPOD = One Application Instance.
- One or more application Domains of One instance of IBM DataPower Gateway Appliance are synchronized by DPOD to another IBM DataPower Gateway Appliance = Two Application Instance.

Currently DPOD is offered in the following packages:

- A single pack Application Instance.
- A single pack Application Instance.

For more information consult the License Information site.

Known Limitations

DPOD Integration with API-C can be applied to only **a single** API Connect Domains per DataPower Device for Firmware lower than 7.6

This limitation is derived from a limitation of the monitored device.

Known workarounds: upgrade to firmware 7.6 or 7.5.2.8.

Changes to Gateway Objects

DPOD requires some configuration changes to at both device and domain levels. These changes include but are not limited to syslog targets.

At the service level - only the optional feature of Extended Transaction requires instrumentation.

To see the full list of changes please look at this table

No support for DHCP

DPOD does not support DHCP network configuration. Please refer to Change Appliance Network Address

Known workarounds:

None.

Operational maintenance plan limitations

DPOD release since v105 few operations maintenance service to assist day to day operational task such backups, configuration sync.

As these features have system wide influence and might affect the availability of the Gateway and services, we provided limitations on the usage of the features.

For backups - see limitations here.

For configuration sync - see limitations here.

For firmware upgrades - see limitations here

Operating System supported locale

The only supported operating system locale definition for DPOD is **en_US.UTF-8** as described in the installation prerequisites.
Object names in non-English languages may be partially supported.

Known workarounds:

None.

Limited functionality is provided when DataPower has language different than English

Choosing language in DataPower will impact your syslog records. This will cause DPOD to provide limited analysis on records that are not in English.

Known workarounds:

Change language of your monitored device to English (en).

Partial Support for Tenant feature

In Firmware 7.6 the tenant module was introduced only to physical appliance type 8436. Currently DPOD is not supporting this monitoring resources of the tenant feature. Capturing transactions on tenants is supported.

Known workarounds:

None. Resolution of this issue is part of the short-term product Roadmap.

WS-M does not capture Multi-Protocol Gateway services payloads for firmware pre 7.5.2 ?

This limitation is derived from a limitation of the monitored device.

Known workarounds:

DPOD version 1.0.2 and IDG Firmware 7.5.2.1 (especially with iFix IT17479: JSON PAYLOAD NOT CAPTURED BY WSM AGENT) should provide this functionality out of the box!

Transactions under the Default domain are not monitored

This limitation is derived from a limitation of the monitored device.

Log targets defined at the Default domain collect all logs from all domains, and currently there is way to apply a filter to the log targets in order to filter out logs from other application domains.

Known workarounds:

There is a workaround, but it only applies if the customer is willing to duplicate all network traffic, or alternatively run transactions only on the Default domain. Please contact support for more details.

Payload size does not include response size (only request size)

At present, monitored devices do not report the front-end response payload size, nor do they report on the back-end request and response.

Known workarounds:

None. Resolution of this issue is part of the product Roadmap.

Limitation on the number of domains that DPOD can monitor on a single Gateway

When you define no custom log targets on the Gateway , the Gateway supports a maximum of 125 domains that DPOD can monitor when the Gateway defines no custom log targets.
Before firmware 7.5.2.4, the Gateway supported 500 log targets. Because the default domain requires 3 log targets and each application domain requires 2 log targets, The Gateway without custom log targets supports a maximum of 248 domains.

After firmware 7.5.2.4 this number were doubled.

When you enable DPOD monitoring, one new log target is added to the default domain and 2 new log targets to each application domain.

Before you can enable DPOD monitoring:

1. View the list of defined domains, to ensure that no more than 125 domains are already defined.
2. Run the **show log-targets** command in Diagnostics mode to determine the number of log targets that are defined.

Known workarounds:

Unless the following calculation results in a positive integer, do not enable DPOD monitoring until you move domains to another Gateway .

```
  Max Log targets per device  - ((domains x 2) - 1) - number_log_targets
```

B2B support is limited

At present, the most important B2B features (e.g. transaction aggregation) are supported. Configuration sampling and specific filtering in dashboards are part of the current version.

Known workarounds:

Upgrade to v1.0.3.0 - Configuration sampling is implemented.

Callable rule invocation appears as a separate transaction

At present, monitored devices do not report the front end response payload size nor do they report on the back-end request and response.

Known workarounds:

Upgrade to v1.0.4.0 - a fix was provided.

Error is not displayed in "Extended transactions"

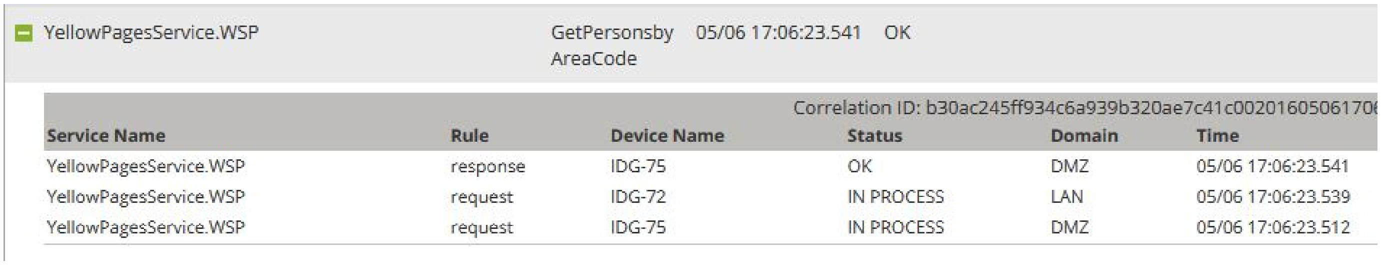
The extended transaction is the only feature of DPOD that involves instrumentation of an XSLT transformation to the Web Service Proxy policy (request / response and error rules).

The instrumentation is integrated by the system only when initiated by the system administrator and not by default.

The behavior when an error is raised by the service (WS-Proxy) depends on the applicable scenario:

No error rule in the service where the error is raised. Previous services are configured with "Process HTTP errors = on"

As there is no error rule, an extended transaction log record will not be generated for the error, and it will not be displayed on the "Extended Transactions" screen.
The extended transaction display will resemble the following (note: one record is missing)



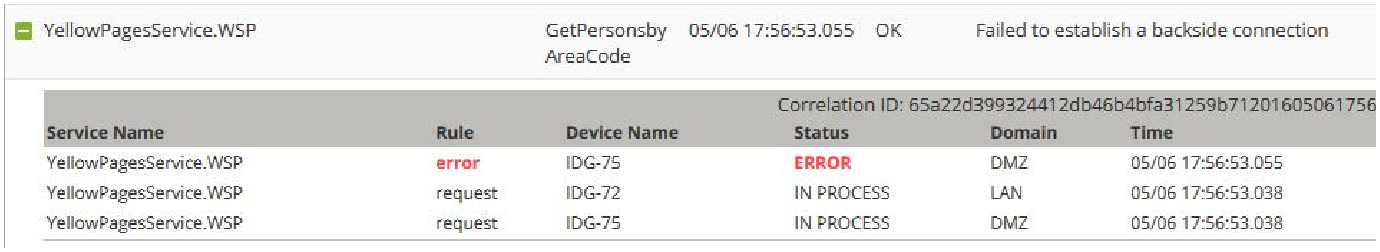
YellowPagesService.WSP	GetPersonsby AreaCode	05/06 17:06:23.541	OK

Correlation ID: b30ac245ff934c6a939b320ae7c41c0020160506170

Service Name	Rule	Device Name	Status	Domain	Time
YellowPagesService.WSP	response	IDG-75	OK	DMZ	05/06 17:06:23.541
YellowPagesService.WSP	request	IDG-72	IN PROCESS	LAN	05/06 17:06:23.539
YellowPagesService.WSP	request	IDG-75	IN PROCESS	DMZ	05/06 17:06:23.512

No error rule in the service where the error is raised. Previous services do have error rule configured

As there is no error rule, an extended transaction log record will not be generated for the error, and it will not be displayed on the "Extended Transactions" screen.
However, as previous services **do** have an error rule, the "Extended Transactions" display will resemble the following:



YellowPagesService.WSP	GetPersonsby AreaCode	05/06 17:56:53.055	OK	Failed to establish a backside connection

Correlation ID: 65a22d399324412db46b4bfa31259b7120160506175б

Service Name	Rule	Device Name	Status	Domain	Time
YellowPagesService.WSP	error	IDG-75	ERROR	DMZ	05/06 17:56:53.055
YellowPagesService.WSP	request	IDG-72	IN PROCESS	LAN	05/06 17:56:53.038
YellowPagesService.WSP	request	IDG-75	IN PROCESS	DMZ	05/06 17:56:53.038

Known workarounds:

None.

The Extended Transaction facility does not support API-Connect

You must NOT run it in API-C / API-M Domains

Note: In some cases, the Extended Transaction is not deployed on MPG services. This is due to the diversity of configuration in these services.

Customers are encouraged to open a PMR (Ticket) and provide the service configuration - so these cases can be addressed and resolved.

Known workarounds:

Similar functionality can be applied with the new non intrusive-extend transaction introduced in v1.0.8.0

More information

For more information and an online demo, please visit IBM

Glossary of Terms

This glossary includes terms, definitions or abbreviation for terms that are commonly used in IBM® DataPower Operations Dashboard.

Letter	Term	Type	Explanation
D	DPOD	abbv.	**D**ata**P**ower **O**perations **D**ashboard
G	Gateway	synonym	**I**BM **D**ataPower **G**ateway
I	IDG	abbv.	**I**BM **D**ataPower **G**ateway
M	Monitored Device		A device attached to DPOD and defined in DPOD Web Console. This will normally be an IDG appliance instance.
O	OS	abbv.	**O**perating **S**ystem

User Guide

Intended Audience

This guide addresses different types of users:

- DataPower Developers
- API Providers
- API Consumers

Built-in User Roles

IBM DataPower Operations Dashboard (DPOD) provides administrators the capability to assign various roles to users. Your administrator will set you up with one or more of the following built-in roles, depending on what tasks you need to perform in DPOD.

- See Security Roles to learn more about the available built-in roles.

Features and Benefits

DPOD provides these features and benefits:

- Self-service port-of-call for developers and service-providers, independent of DataPower administrators
- Multiple service dashboards providing at-glance overview of the system’s status from various views including services, devices, domains and transactions.
- Drill-down capabilities into a system’s transactions and assets, to help pinpoint problems for investigation
- Means to investigate errors across the system
- Aids for debugging failed transactions or services, allowing full-data traces
- Robust transactions log views
- Near real time monitoring

By using DPOD you can effectively identify and resolve performance or security related issues that have occurred on your system.
DPOD provides various views and tools that let you gauge the system’s health, identify errors and investigate their causes.

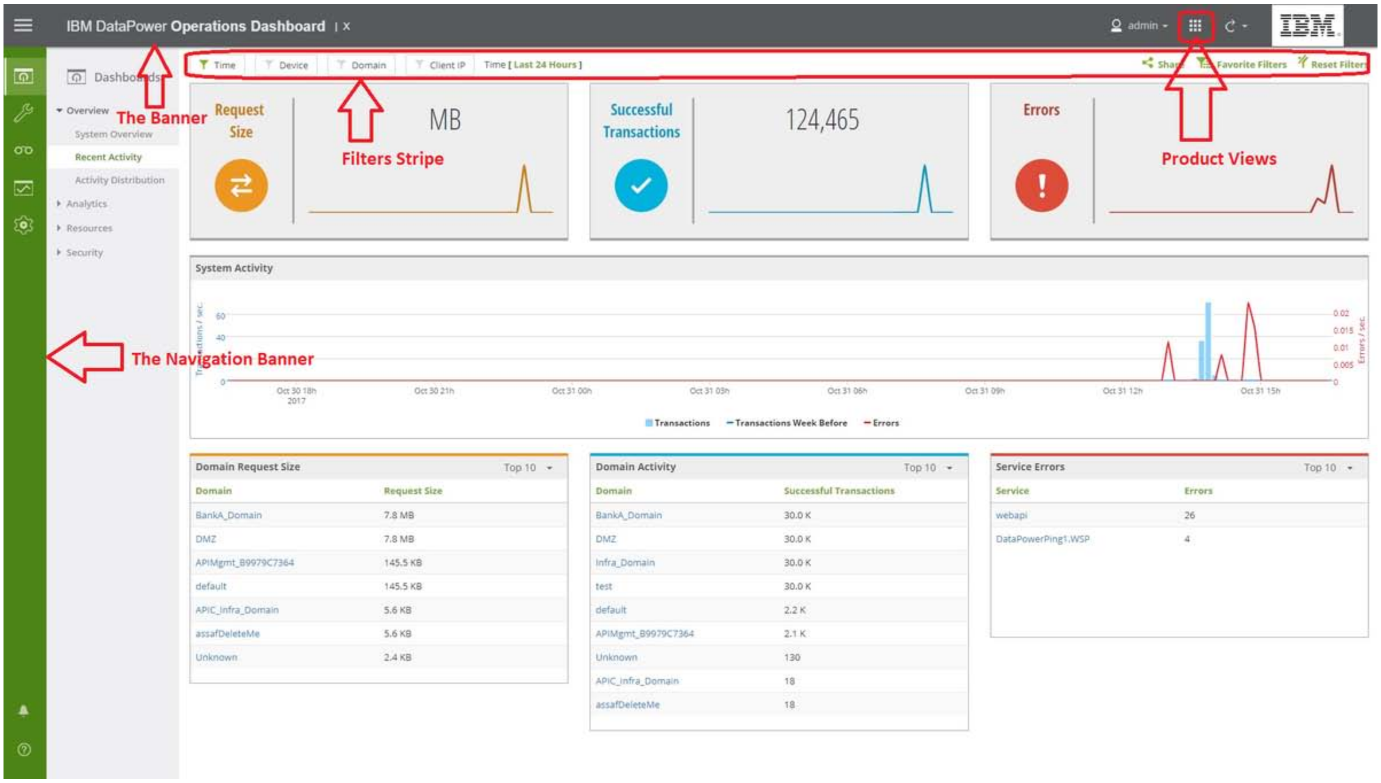
Before You Start

To use DPOD, your administrator should set you up with a login to the system.

- The login credentials provided must belong to at least one built-in role.
- DPOD's display changes according to the role(s) provisioned to you. Different roles have access to different menu items, dashboards and transaction data.
- Please ensure you meet all of DPOD's Client-Side Requirements

Web Console

The screenshot below provides an overview of DPOD's Graphical User Interface, where the various parts are visible.



Domain Request Size — Top 10

Domain	Request Size
BankA_Domain	7.8 MB
DMZ	7.8 MB
APIMgmt_B9979C7364	145.5 KB
default	145.5 KB
APIC_Infra_Domain	5.6 KB
assafDeleteMe	5.6 KB
Unknown	2.4 KB

Domain Activity — Top 10

Domain	Successful Transactions
BankA_Domain	30.0 K
DMZ	30.0 K
Infra_Domain	30.0 K
test	30.0 K
default	2.2 K
APIMgmt_B9979C7364	2.1 K
Unknown	130
APIC_Infra_Domain	18
assafDeleteMe	18

Service Errors — Top 10

Service	Errors
webapi	26
DataPowerPing1.WSP	4

Figure 1 - DPOD's Graphical User Interface

The sections below describe the navigation controls inside DPOD

- The Banner
- The Navigation Bar
- Product Views
- Filters Stripe
- Drilling Down
- Alerts and Feedback Messages
- Export Data to CSV

The Banner

The Banner

The banner at the top of DPOD's GUI provides quick access to:

The Navigation Bar Expand Button

Which can be used to expand the Navigation Bar and show captions for the icons on it.

The Service Center name

Which is set by DPOD’s administrator, and allows different sessions for different topologies.

The logged in user controls

The logged in user controls

Lets the logged in user change preferences, change password and sign out.

The Product View Icon

Switch between DataPower and API Connect product views

The Auto-reload list

Lets users configure the interval DPOD uses to auto-reload the data displayed.

- User Preferences
- Change Password Page
- Signing Out
- About DPOD
- Auto Reload Interval

User Preferences

The user preferences can be accessed by clicking the user name on the Banner, and selecting **Preferences** from the drop-down list.

Click on the Edit button to configure DPOD's views defaults.

The following user-editable preferences are available

Preference Name	Behavior
Theme	DPOD provides three User Interface themes. You may choose a light, dark or elegant theme for DPOD's display.
IDG Home Page	Lets you configure the page DPOD loads when you log in to the system in IDG view mode or when switching to IDG view mode and when an auto-navigate Home Interval is used
APIC Home Page	Lets you configure the page DPOD loads when you log in to the system in APIC view mode or when switching to APIC view mode and when an auto-navigate Home Interval is used
Auto-reload Interval	When used, DPOD will automatically reload its display according to the interval selected: • Every 10 Seconds • Every 30 Seconds • Every 5 Minutes • Or manually (Never auto-reload) The auto-reload interval selection can also be accessed directly from the banner, by clicking the auto-reload icon
Auto-navigate Home Interval	Number of seconds of inactivity after which DPOD will reload the home page. If set, DPOD will navigate the user back to the defined home page after a period of inactivity. An example of where this is useful would be for NOC display terminals
Internal Alerts Message Interval	This option is only displayed for administrators. How often internal health notifications will be displayed The default value is every 1 minute, you can turn the notification off (not recommended)
Store Status Message Interval	This option is only displayed for administrators. How often the Store status message should be displayed. The store status message shows the date of the earliest syslog document stored in DPOD. The default value is every 8 hours, you can turn the notification off.
Default Device Filter	You may enter device name(s) here to automatically set a default Device Filter value for all views.
Default Domain Filter	You may enter domain name(s) here to automatically set a default Domain Filter value for all views.
Default Service Filter	You may enter service name(s) here to automatically set a default Service Filter value for all views.

Change Password Page

> This page is only available for environments without LDAP

Enter the new password twice and press "Update" to update your password.

Signing Out

To sign out of DPOD, click the username on the banner and then select the Sign Out link.

About DPOD

To access DPOD’s About pop up, click the user name on the banner and select the **About** option.
The About pop up contains general information about DPOD’s server, and several links to agreements and notices.

Auto Reload Interval

Clicking the ↻ icon on the banner opens a drop-down menu that allows you to configure DPOD’s auto-reload interval for the data displayed in the main window.
You may select one of the pre-configured intervals of

- 10 seconds,
- 30 seconds
- 5 minutes
- Manual: opt for never to auto-reload, by selecting this option.

Auto-reload works well for hands-off displays (e.g. on a large screen in the NOC) - but is not suitable for investigation or debug scenarios.

The Navigation Bar

The navigation bar along the left side provides access to the main actions available in DPOD. This area contains the following controls:

Icon Link	Purpose
⏲	Dashboards opens the available dashboards list in the navigation panel
🔧	Investigate provides access to the investigation view, where you can focus on troublesome areas and investigate causes
∞	Explore provides access into the Service Configuration view, where you can explore the various services deployed and their attributes
✓	Reports provides access to DPOD’s reports tool suite

The bottom part of the navigation bar shows the following toggles:

Icon Link	Purpose
🔔	Shows or hides DPOD's recent UI messages. The recent messages will clear upon sign-out or page refresh and are not shared between different users
?	Shows or hides DPOD’s context-sensitive help for the User Interface. Activating the toggle will display small ? icons over screen elements. Hover on an icon to display the context-sensitive help related to the element. Click the Help Toggle again to hide all icons.

NAVIGATION MENU

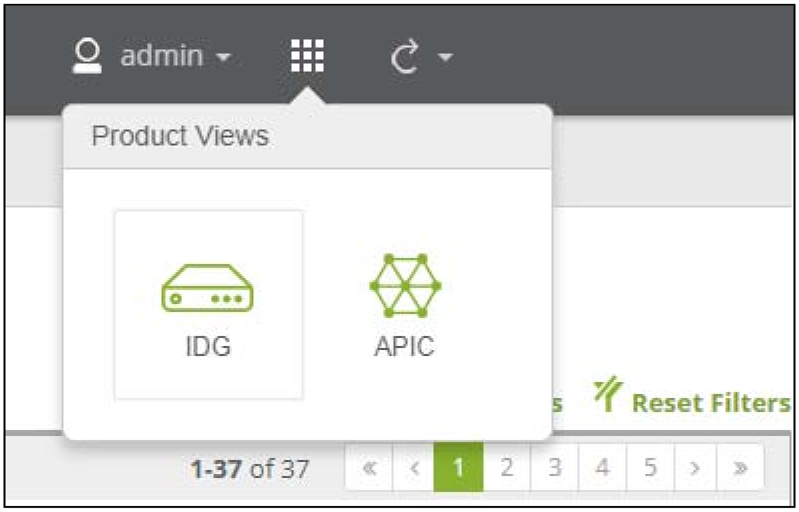
When the user selects the Dashboards link, DPOD displays the vertical navigation menu immediately to the right of the navigation bar. The navigation menu lists the various dashboards available for viewing.

Product Views

Click on the Product Views icon ▦ to switch between DataPower and API Connect view modes.

The reports and manage menus are identical and shared between the two product views.

The dashboards and investigate menus contain different items and information for each product view

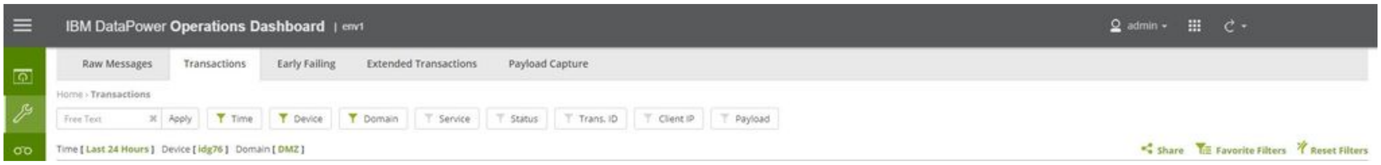


If and admin enabled "Show Custom Transaction View Selection" in system parameters, the "Custom TX View" checkbox will be also displayed. Click it to toggle between syslog and custom transaction view in the DataPower Transactions view.

Filters Stripe

The Filters Stripe comprises a set of filter elements that let you control the attributes of the information displayed in the main window.
The Filters Stripe is displayed at the top of the main window, for all views except the Reports view.

USING THE FILTERS STRIPE



To filter the information displayed, click on the filter element required. Performing this action will open a list containing the filter options. You may then click the filtering option you want to apply. Alternatively, you may type in a value (e.g. a specific interval in the **Time** filter or a specific device name in the **Device** filter) and click ‘Apply’. (You do not need to click ‘Apply’ if you select one of the options already displayed).

Some filters allow multi-selection by typing in a comma-separated list of values.

You may combine several filters simultaneously. DPOD will alter the displayed information to reflect it.

Active filters will show the icon next to them, inactive filters will show the icon.
Additionally, the filter’s name and value will be added to the active filters display – a line of text immediately underneath the filter elements.

EXAMPLE

When no filters are applied to DPOD’s display. Click the **Time** *filter element* and then click to select the **‘Last Hour’** option.

The **Time** filter’s icon will be highlighted and the text **Time [Last Hour]** will appear underneath the Filters Stripe.

DPOD retains your active filters as you move through its various views. This allows you, for example, to identify a rogue transaction through the Service Latency dashboard, and then click on the Troubleshoot view to explore the filtered data further.

To disable a filter, click its *filter element* and select ‘clear’ from the bottom of the list. Alternatively use the ‘Reset Filters’ link found at the far right of the active filters display.
This will reset the display to the default filter which is **Time [Last 24 Hours].**

TOOLS

Three tools are available on the bottom-right side of the filters stripe:
Share - allows the user to share the current page, including any active filters
Favorite Filters - allows the user to save the current set of active filters or load and apply previously saved sets
Reset Filters - reset all the filters to their initial state

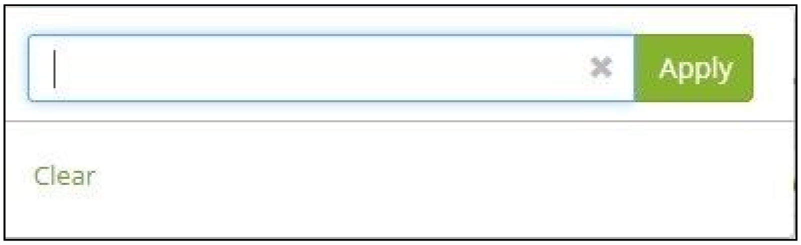
Filters

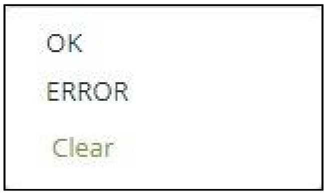
Filters change the currently displayed data. They can be used, for example, to display only certain transaction IDs, Devices or Domains.

Some filters provide a list of optional values. To use those values, start typing in the input box to activate the auto-complete within the filter. Alternatively, you may scroll the value list using the keyboard arrow keys and select values by pressing enter.

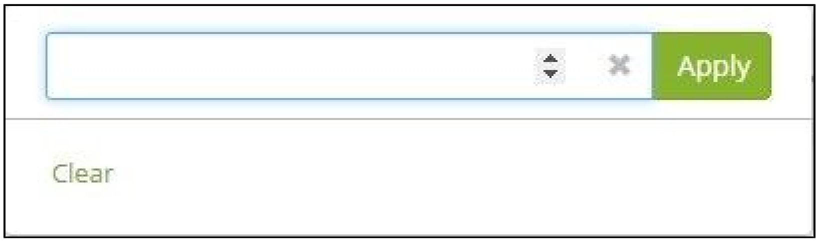
Single Value Filters

Enter a single value in the input field and click apply or select a single value from the list (when available)



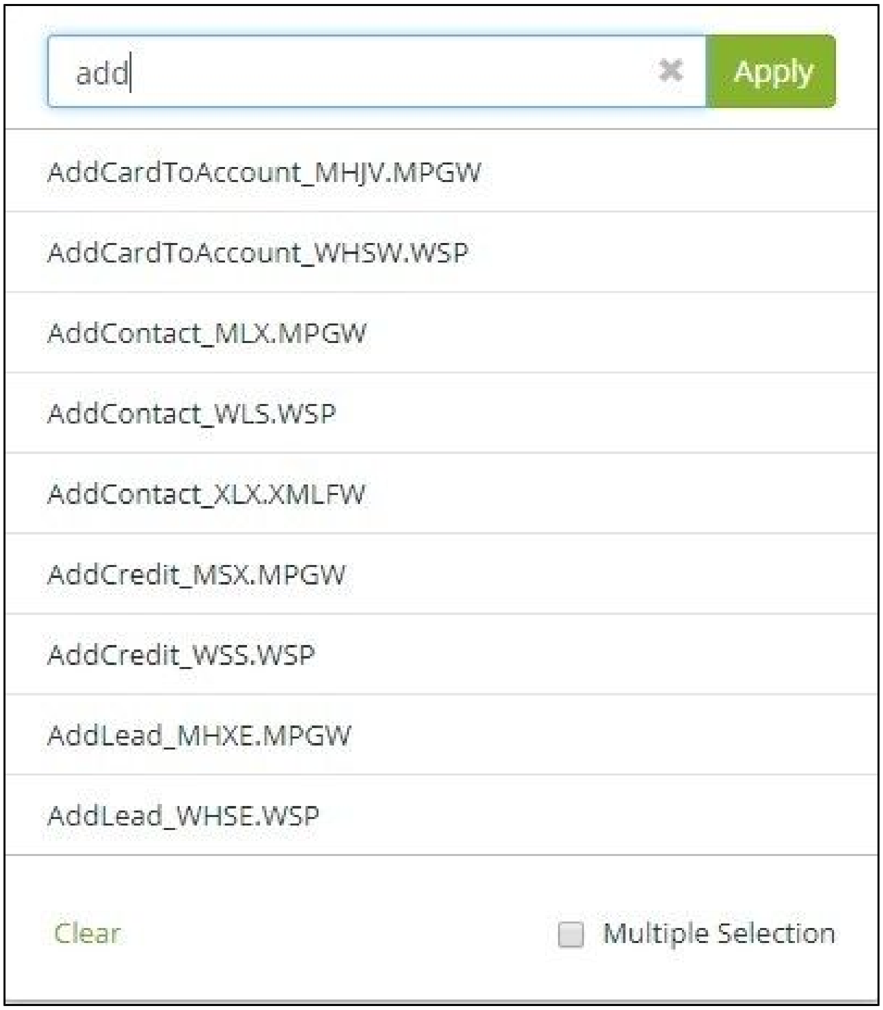


Some filters (for example, minimum latency), will only accept numerical input



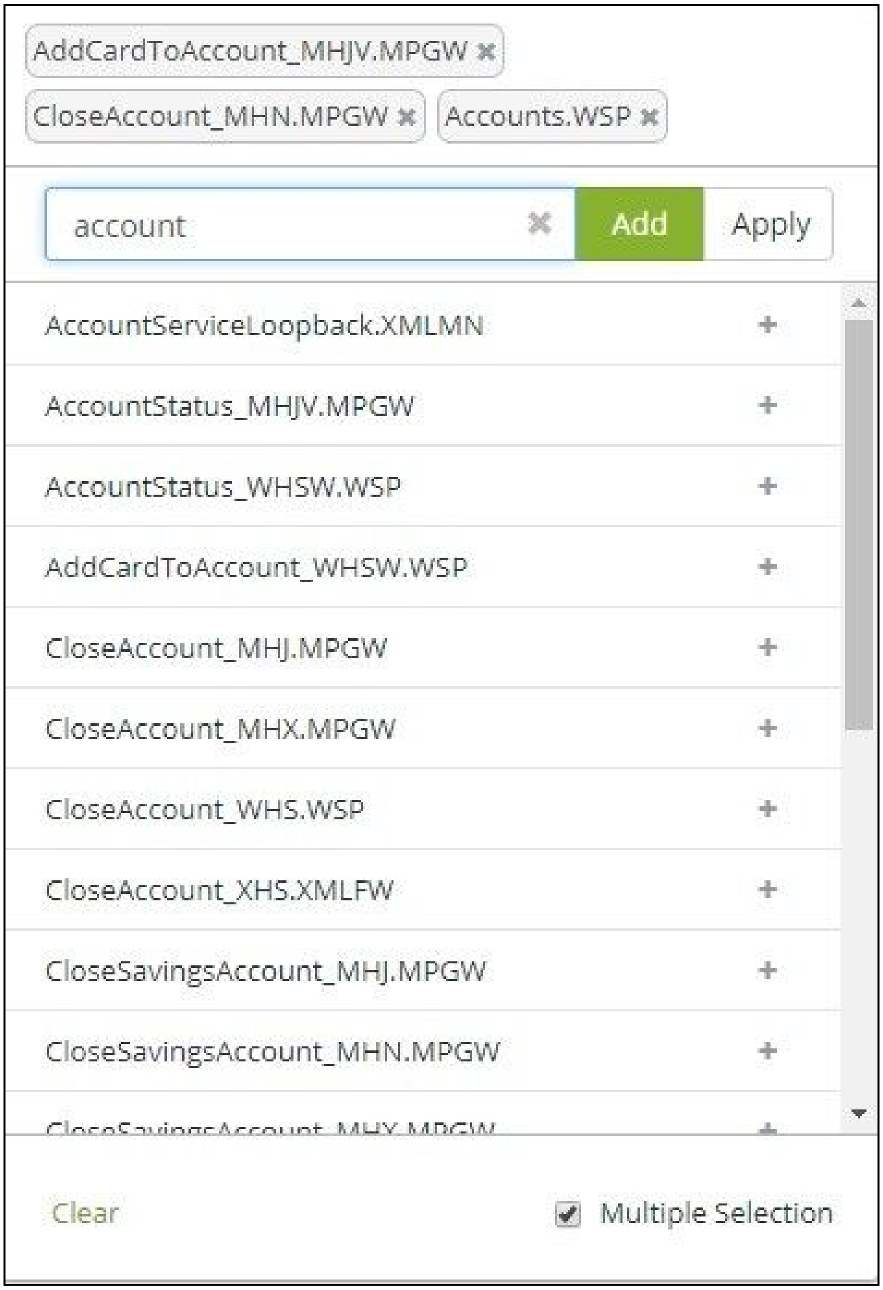
Multiple Value Filters

Multiple Value Filters start by default in "Single Selection" mode, select a value from the list to choose this value and close the filter.
You may type anything into the input box. Filters are not restricted to the list of available values.



add

Click on the "Multiple Selection" checkbox on the bottom-right to show the multiple selection panel.
In Multiple Selection mode, click on a value to add it to the selection list (shown on top), click on a value in the selection list to remove it.



AddCardToAccount_MHJV.MPGW ✖

CloseAccount_MHN.MPGW ✖ Accounts.WSP ✖

account ✖

☑ Multiple Selection

Add
Apply
AccountServiceLoopback.XMLMN +
AccountStatus_MHJV.MPGW +
AccountStatus_WHSW.WSP +
AddCardToAccount_WHSW.WSP +
CloseAccount_MHJ.MPGW +
CloseAccount_MHX.MPGW +
CloseAccount_WHS.WSP +
CloseAccount_XHS.XMLFW +
CloseSavingsAccount_MHJ.MPGW +
CloseSavingsAccount_MHN.MPGW +
CloseSavingsAccount_MHX.MPGW +
Clear

Click on Apply to apply the current selection.
Click outside the filter or on the filter's title to close the filter without applying.
Click the "Multiple Selection" checkbox again to return to single selection mode.

AVAILABLE FILTERS

The following table lists the available filters within DPOD.
Most sections of DPOD display only a subset of this list, as applicable to the data displayed in different sections.

Filters in IDG View

Filter Name	Functionality
Application Data	Visible on the Deprecated Extended Transactions screen only, it is used to search user data. The use of this filter requires XSLT modification
B2B Message ID B2B From Partner ID B2B To Partner ID B2B From Partner Profile B2B To Partner Profile	Visible in the Raw Message screen only. The B2B Message ID, From Partner ID, To Partner ID, From Partner Profile and To Partner Profile.
Category	Only show messages of the selected category or categories. Valid values: The filter's list is pre-populated with some built-in values. Users may enter their own values as free text
Cause	Visible in the Restarts dashboard only. The restart cause (device initiated, user initiated, etc.)
Catalog Name	API Connect dashboards only.
Client IP	Only show messages and transactions originating on one or more client IPs. The client IP may be either the origin of the message or the load balancer. Valid values: Valid IP Addresses
Corr. Id	Only show information related to one or more correlation ids. This filter only applies to the Deprecated Extended Transactions page. Valid values: Correlation ids of extended transactions.
Device	Only show information related to the selected device(s).
Domain	Only show information related to the selected domain(s). Asterisk wildcard is supported. e.g. "Prod*" will match all domains that starts with "Prod".
Downtime Started	Visible in the Restarts dashboard only. The estimated time where the device was not available
Error Message	Only show transactions that failed, where the error message contains the term entered into the input box for this filter. Valid values: Free text
Free Text	Enter a value to search in multiple fields at once (depends on the page where the filter exists). Starting to type in the filter will highlight (using a shadow) all other filters that will be searched for the value entered in the Free Text filter. For example, in DataPower Transactions, the Device, Domain, Service, Transaction ID and Client IP information will be searched for the value entered in the Free Text filter. All values are case sensitive, except for the raw messages' message content (which is case insensitive).
Front-Side Handler	Only show services going through the specific Front-side handler(s). Valid values: • Front Side Handlers in the system (Configuration Only)
Front URI	The URL the service exposes (Configuration Only)
Global Trans. ID	The Global Tansaction ID
In URI	Visible on Extended Transactions and Service URI Calls only. The URI that clients use to invoke transactions.

In URL	Visible on Deprecated Extended Transactions and Service URL Calls only. The URL that clients use to invoke transactions.
Message	
Message Code	Message code as reported from a log target of a monitored device.
Min Elapsed	Filter the displayed transactions by minimum elapsed time (in ms). Valid values: Non-negative integers
Min Request	Filter the displayed transactions by minimum request size(in bytes). Valid values: Non-negative integers Available since IDG firmware 7.6.0.8 and 7.7.1.2 for transactions of traditional IDG services
Min Response	Filter the displayed transactions by minimum response size(in bytes). Valid values: Non-negative integers Available since IDG firmware 7.6.0.8 and 7.7.1.2 for transactions of traditional IDG services
Obj. Name	Object Name as reported from a log target of a monitored device. Normally contains service Name or front side handler
Obj. Type	Object Type as reported from a log target of a monitored device.
Operation	Service Operation name - only applies for Web-Service Proxy service type.
Out URL	Visible on Extended Transactions only. The URL that the transaction invoked at the back end.
Payload	WS-M payload recorded on monitored devices.
Service	Only include transactions on the selected service(s). Enter either a single service name or multiple names as a comma-separated list. Valid values: Any service name(s) in the system The available values list will change according to the context: In the Investigate section - Raw Messages, Transactions or Extended Transactions pages, the list of values will only show services that actually run on the monitroed devices. In the Explore section - Service Configuration and DevOps services portal, the list of values will show all the services on the monitroed devices, even if they never executed. You may, enter any value into the filter, even if it doesn't appear in the list of available values.
Service Type	Multi Protocol or Web Service Proxy (Configuration Only)
Severity	Severity as reported from a log target of a monitored device.
Status	Only include transactions with the selected status(es). Valid values: • OK • ERROR • IN PROCESS

Time	Filter display by time interval. Valid values: - Last 5 minutes - Last 10 Minutes - Last 15 Minutes - Last 30 Minutes - Last Hour - Last 24 Hours - Last 7 Days - Last 30 Days - Today (Since midnight) - This Week (Since midnight on Monday) - This Month (Since midnight on the first day of the month) - Yesterday (24 hours ending at midnight of previous day) - Last Week (7 days ending at midnight of previous day) - Last Month (Midnight 1st of previous month to Midnight 1st of current month) - User-defined Interval
Trans. Direction	Filter display by the transaction's direction. Valid values: - Request - Response - Error
Trans. ID	Filter display by the id(s) of one or more transactions. Valid values: Transaction ids

Additional Filters in APIC View

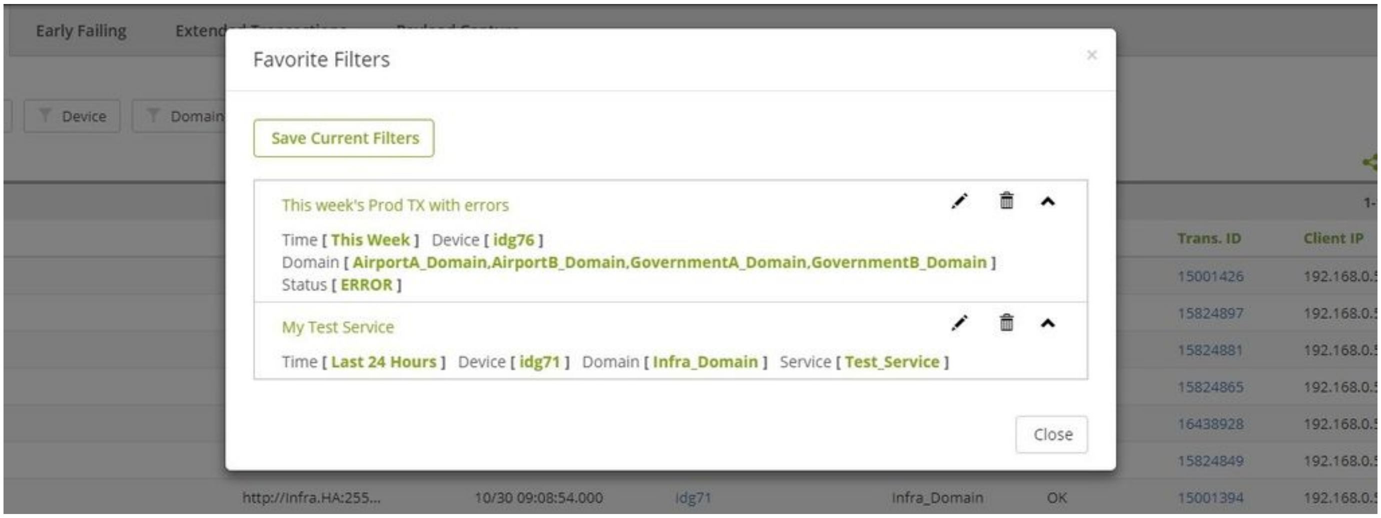
Filter Name	Functionality
Catalog	Filter the displayed transactions by the name of the catalog that was used during the API call.
Space	Filter the displayed transactions by the name of the space that was used during the API call.
Product	Filter the displayed transactions by the product name that was consumed by the API call.
Plan	Filter the displayed transactions by the name of the plan that was used during the API call.
API Name	Filter the displayed transactions by the name of the API that was activated.
API Version	Filter the displayed transactions by the version of the API that was activated.
App Name	Filter the displayed transactions by the name of the consumer application that made the API call.
HTTP Method	Filter the displayed transactions by the HTTP method that was used in the API call HTTP request.
Path URL	Filter the displayed transactions by the URL that was activated by the client.
FE HTTP Res. Code	(Front-End HTTP Response Code) Filter the displayed transactions by the HTTP response code that the APIC sent back to the client.
BE HTTP Res. Code	(Back-End HTTP Response Code) Filter the displayed transactions by the HTTP response code that the APIC received from the back-end.
Consumer Org Name	Filter the displayed transactions by the consumer organization name that the client who activated the API call belongs to.
Client ID	Filter the displayed transactions by the ID of the client that activated the API call. Client IDs are generated by the API Management server during client registration.
Client IP	Filter the displayed transactions by the client IP address or load balancer address of the consumer that made the API call.
OAuth Scope	Filter the displayed transactions by the scope of the OAuth token that was delivered by the client in the API call.

OAuth Resource Owner	Filter the displayed transactions by the resource owner of the OAuth token that was delivered by the client in the API call.
OAuth Token Valid From	Filter the displayed transactions by the time that the OAuth token is valid from.
OAuth Token Valid Until	Filter the displayed transactions by the time that the OAuth token is valid until.
Min Request Latency	Filter the displayed transactions by the minimum time it took to process the request (in ms).
Min Response Latency	Filter the displayed transactions by the minimum time it took to process the response (in ms).
Min Back-End Latency	Filter the displayed transactions by the minimum time it took to wait for the backend server to reply (in ms).
Min Total Latency	Filter the displayed transactions by the minimum time that the API transaction took till a response was returned to the client (in ms).
Min Request Size	Filter the displayed transactions by the minimum size of the request.
Min Response Size	Filter the displayed transactions by the minimum size of the response.
Error Reason	Filter the display to only show transactions that failed, where the error reason contains the term typed in the input box for this filter.
Error Message	Filter the display to only show transactions that failed, where the error message contains the term typed in the input box for this filter.
Policy Name	Filter the displayed transactions by the policy name of the element in API diagram/assembly.

Favorite Filters

The favorite filters window allows the user to store and load filter sets.

> the saved filter sets are **not** shared between dashboards or between users



Favorite Filters

This week's Prod TX with errors

Time [This Week] Device [idg76]
Domain [AirportA_Domain,AirportB_Domain,GovernmentA_Domain,GovernmentB_Domain]
Status [ERROR]

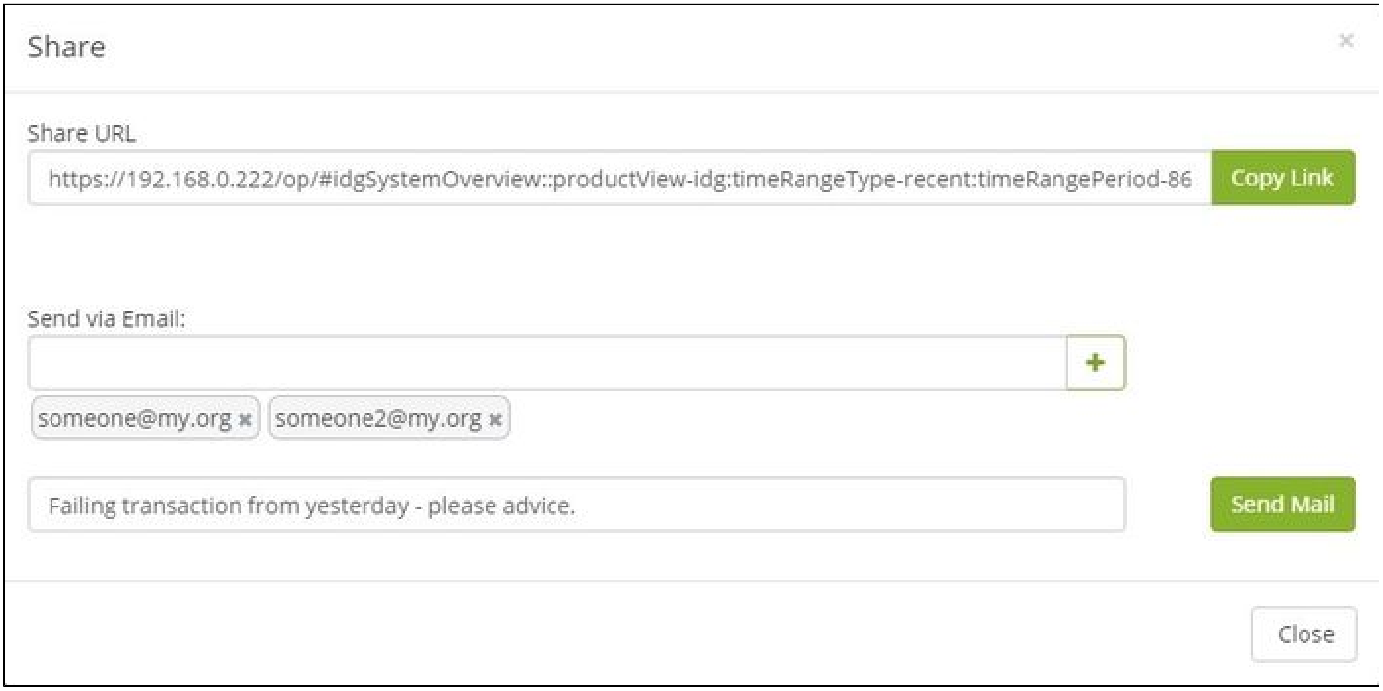
My Test Service

Time [Last 24 Hours] Device [idg71] Domain [Infra_Domain] Service [Test_Service]

Click "Save Current Filters" to save the current dashboard's active filters.
Click on the saved filters name to load them into the dashboard.

Share

Click the Share button (at the bottom-right corner of the Filters Stripe) to open the Share window



Share

Share URL

https://192.168.0.222/op/#idgSystemOverview::productView-idg:timeRangeType-recent:timeRangePeriod-86

Send via Email:

someone@my.org someone2@my.org

Failing transaction from yesterday - please advice.

The share window contains two parts:

Top part - Click on "Copy Link" to copy the current link to the clipboard, you may also copy the link directly from the input box.

> In some browsers, you may need to change the browser's setting to allow DPOD to access the clipboard.
> For example, in Internet Explorer you will need to enable "Allow Programmatic clipboard access" in the security settings.

Bottom part - Enter email recipients (and an optional message) and click on "Send Mail" to send them an email with the link to DPOD.
In order to send an email, the mail system parameters need to be configured - see System Parameters List for more information

> Accessing DPOD from a shared link will require login
> There is no way to access DPOD's data annonymously, without a valid DPOD user

Configuring Custom Share Email Format

You can replace DPOD's default email format with your own email format:

1. Create a plain-text file that contains your new template.
   The first line should contain the email's title
   Other lines should contain the email's body, you may enter HTML tags such as <br>
   The following symbols will be replaced in the title/body:

Where	Symbol	Meaning
Title and Body	%product	The product's name (=DPOD)
Title and Body	%1	The sending user's name
Body	%2	The URL to share
Body	%3	The user comment, if any, as entered in the Share window

2. Login to DPOD via ssh
3. Upload the file to /app/custom/template/shareMailTemplate.txt (you may need to create the folder if it does not already exist)

Drilling Down

DPOD’s display contains multiple graph widgets which visualize system information on the screen.

Depending on your system configuration, some of these widgets may contain a lot of information.

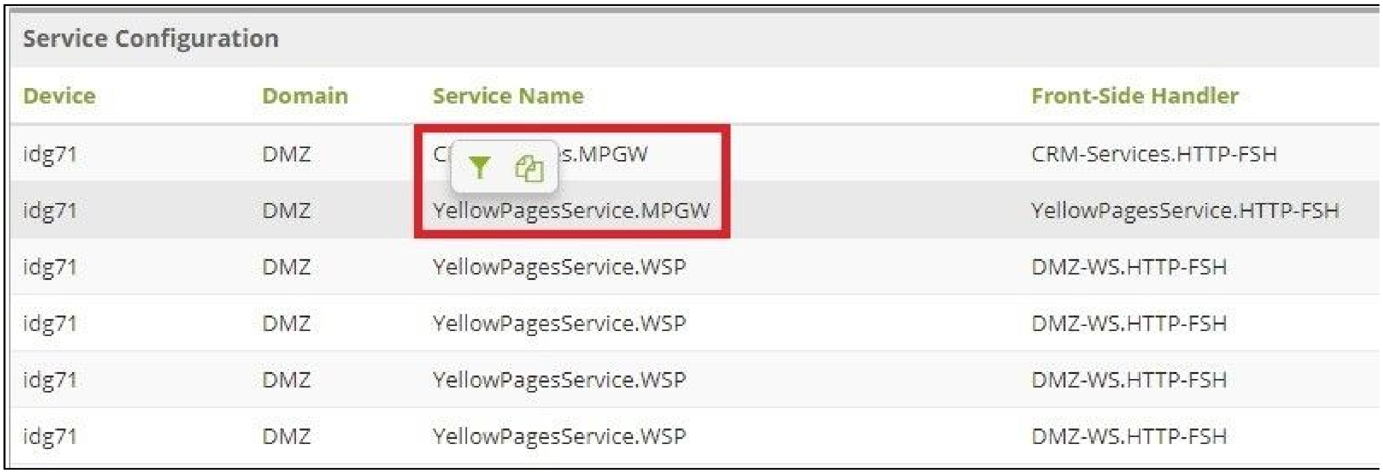
DPOD provides numerous methods to control the amount of data displayed.

1. The filters in the Filters Stripe
2. The captions underneath the graphs are clickable, and may be used in much the same way the *Filter Elements* are used.
   Click a caption to apply a filter based on the caption.
3. The graphs themselves are clickable. You may click an area on the graph and drag right or left to highlight and select a specific time interval.
   DPOD will update the graph to only show data inside the selected interval.

THE CONTEXT MENU

> For DPOD v1.0.6 - The following feature is only available in the Service Configuration page

Click anywhere on the row to drill down - in the service configuration page, drilling down will show the service configuration of the service.
Hover the mouse for half a second over a data item and the context menu will open automatically.



Service Configuration

Device	Domain	Service Name	Front-Side Handler
idg71	DMZ	C s.MPGW	CRM-Services.HTTP-FSH
idg71	DMZ	YellowPagesService.MPGW	YellowPagesService.HTTP-FSH
idg71	DMZ	YellowPagesService.WSP	DMZ-WS.HTTP-FSH
idg71	DMZ	YellowPagesService.WSP	DMZ-WS.HTTP-FSH
idg71	DMZ	YellowPagesService.WSP	DMZ-WS.HTTP-FSH
idg71	DMZ	YellowPagesService.WSP	DMZ-WS.HTTP-FSH

The context menu contains two buttons:

Add to filters - will add the value to the current filter set
Copy to clipboard - will copy the value to the clipboard

> In some browsers, you may need to change the browser's setting to allow DPOD to access you clipboard.
> For example, in Internet Explorer you will need to enable "Allow Programmatic clipboard access" in the security settings.

Alerts and Feedback Messages

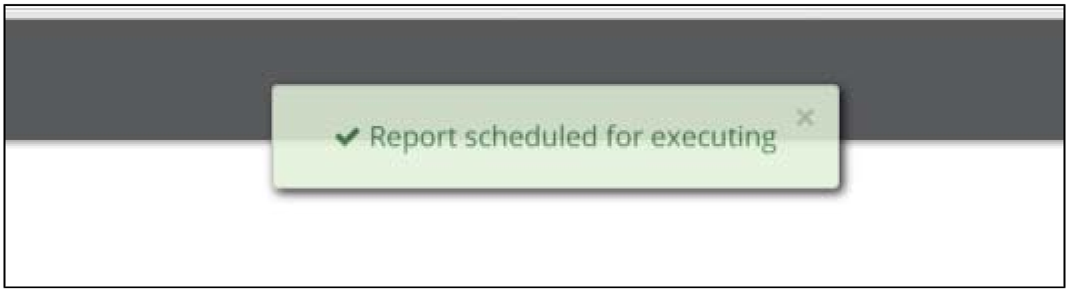
DPOD provides user feedback by means of Feedback Messages. These appear to drop down from the top of the screen.

You may dismiss the messages by clicking the x icon on the top right of a message. Alternatively - messages drop up and out after a set amount of time.

You can view all recent messages in the notification window (click on the 🔔 icon on the bottom-left to open the window) the recent messages window will clear upon page refresh or logoff.

SUCCESS / INFORMATIVE MESSAGES

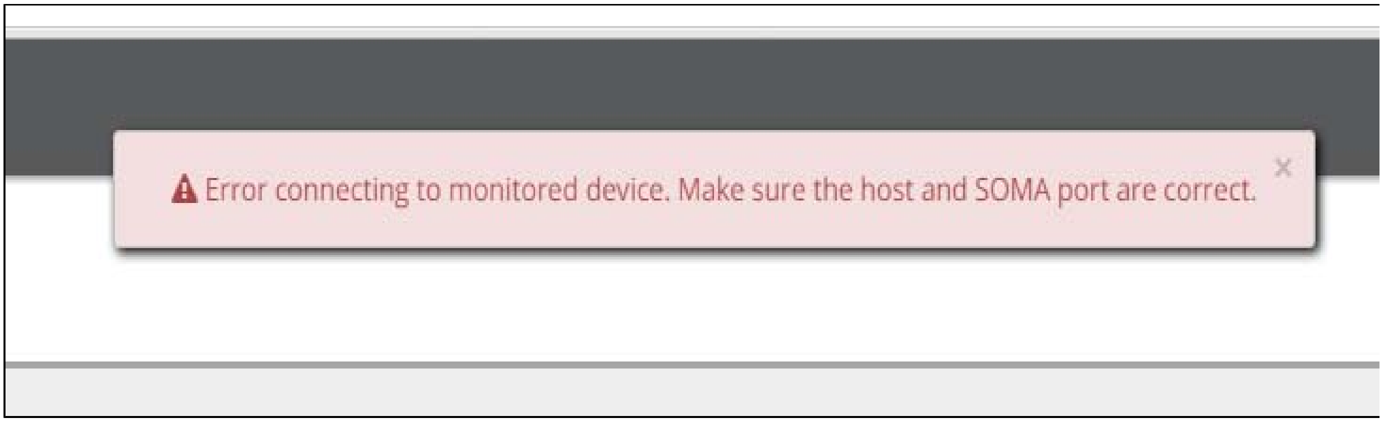
Green messages provide informative indication on completion of a successful operation such as configuration update or a report successfully scheduled.



✓ Report scheduled for executing ×

ERRORS

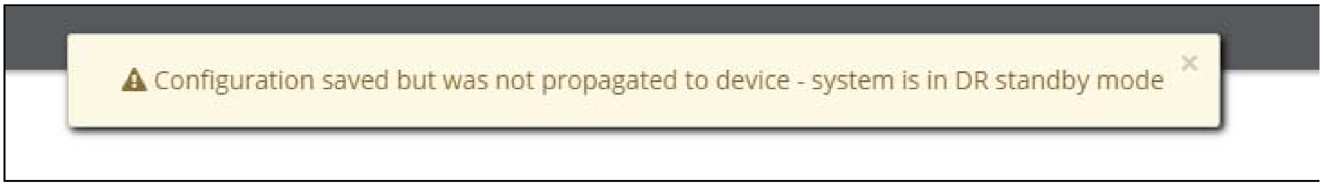
Red messages provide information on an erroneous operation or situation. The error message will usually contain a hint or directive to the user with a suggestion to fix the error.



⚠ Error connecting to monitored device. Make sure the host and SOMA port are correct. ×

WARNING MESSAGES

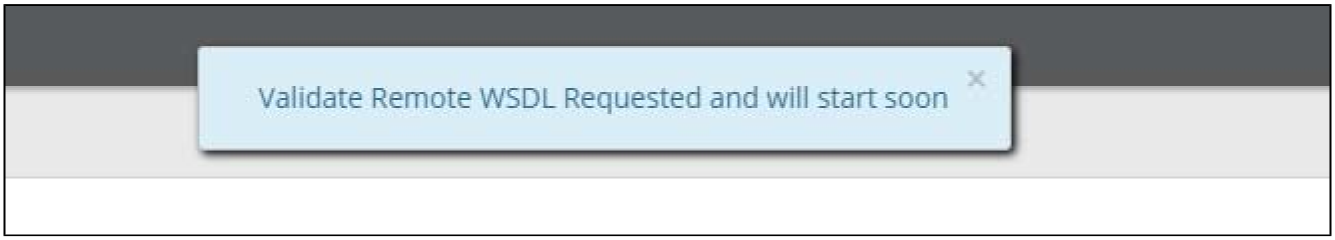
Yellow messages provide information about actions that were executed successfully, but with some limitation or addition info the user needs to note.



⚠ Configuration saved but was not propagated to device - system is in DR standby mode ×

GENERAL MESSAGES

Blue messages provide general information on an operation or situation.



Validate Remote WSDL Requested and will start soon

AUTOMATIC DISMISSAL

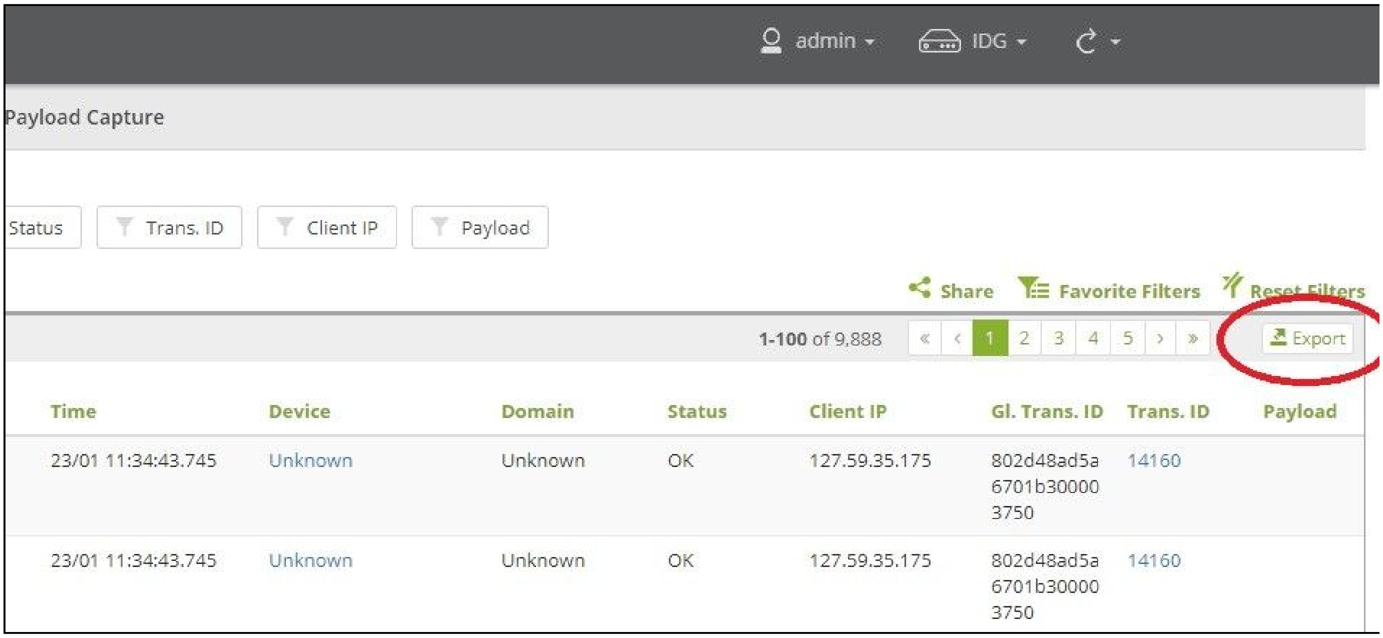
Messages are automatically dismissed after a set number of seconds:

Message Type	Dismissed After
Success / Informative	5 Seconds
General	5 Seconds
Warning	15 Seconds
Error	15 Seconds

Export Data to CSV

Most of the dashboards allow to export the data as CSV (comma separated)
Click the Export button and the download should start automatically after a few seconds.

> This feature is available for Chrome browser and latest version of Firefox
> DPOD will export up to 1000 rows of data



Payload Capture

1-100 of 9,888

Time	Device	Domain	Status	Client IP	Gl. Trans. ID	Trans. ID	Payload
23/01 11:34:43.745	Unknown	Unknown	OK	127.59.35.175	802d48ad5a6701b300003750	14160	
23/01 11:34:43.745	Unknown	Unknown	OK	127.59.35.175	802d48ad5a6701b300003750	14160	

Admin Console

The screenshot below provides an overview of DPOD's Graphical Admin User Interface, where the various parts are visible.

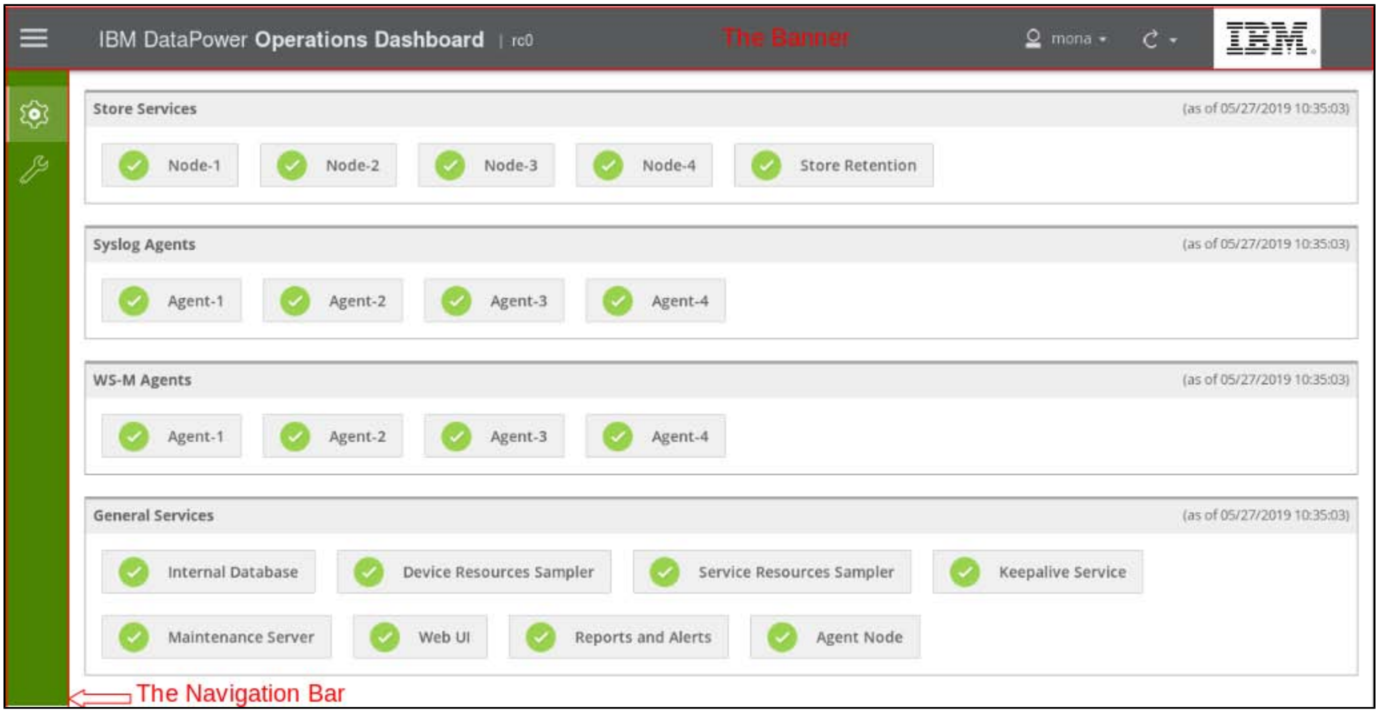


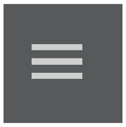
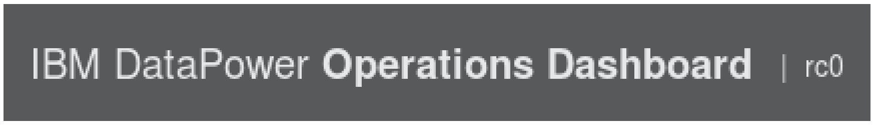
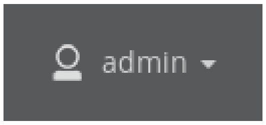
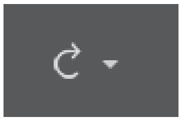
Figure 1 - DPOD's Graphical Admin User Interface

The sections below describe the navigation controls inside DPOD

- Admin Console's Banner
- Admin Console's Navigation Bar
- Admin Console's List Of Utilities

Admin Console's Banner

The banner at the top of DPOD's Admin GUI provides quick access to:

Icon	Purpose
	**THE NAVIGATION BAR EXPAND BUTTON** • Which can be used to expand the Navigation Bar and show captions for the icons on it.
 IBM DataPower **Operations Dashboard** | rc0	**THE SERVICE CENTER NAME:** • Which is set by DPOD's administrator, and allows different sessions for different topologies.
 admin	**THE LOGGED IN USER CONTROLS:** • Shows current logged in user name. • Allows changing of local admin's password. • Log off button
	**THE AUTO-RELOAD LIST:** • Lets users configure the interval DPOD uses to auto-reload the data displayed.

Admin Console's Navigation Bar

The navigation bar along the left side provides access to the main actions available in DPOD. This area contains the following controls:

Icon Link	Purpose
⚙	STATUS Opens the service status screen that shows all the application services configured on current installations and their status.
🔧	UTILITIES Provides access to graphical user interface for common administrations task. such as starting the must gather archive process and accessing must gather file and configuring the product to work with LDAP user registry. Further information can be found in Admin Console's List Of Utilities

NAVIGATION MENU

When the user selects the Dashboards link, DPOD displays the vertical navigation menu immediately to the right of the navigation bar. The navigation menu lists the various dashboards available for viewing.

Admin Console's List Of Utilities

Utility	Purpose
Application	
Stop/Start Services	***Location: Admin Console Utilities Application Stop/Start Services*** Use this utility to stop or start services. When **starting** a service with dependencies, all dependencies will be started as well. When **stopping** a service with dependencies, all dependent services will be stopped as well. The dependency order between services is 1. Configuration database 2. Store services 3. Syslog agents 4. WS-M agents 5. Store retention service 6. Device and service resource samplers 7. Keepalive service and the maintenance service 8. Web UI 9. Reports and alerts 10. Agent node
Download Must Gather	***Location: Admin Console Utilities Application Stop/Start Services*** Use this utility to generate a compressed archive file containing information and logs in /tmp directory.
Change Agent TCP Port	***Location: Admin Console Utilities Application Change Agent TCP Port*** Syslog and WS-M agents listen to predefined TCP ports: Syslog agents: 60000-60009 WS-M agents: 60020-60029 Use this utility to change these default settings. Please make sure the required network connectivity (e.g. firewall rules) is available between monitored devices and the agents.
Backup Application	***Location: Admin Console Utilities Application Backup*** Use this utility to backup the software, static configuration and user configuration data (internal DB).
LDAP Configuration	***Location: Admin Console Utilities Application LDAP Configuration*** Use this utility to configure the system to authenticate users with LDAP user registry or local user registry based on system internal database. Available options: • Test LDAP Configuration: Only test if parameters file is valid and the application can connect to LDAP. • Update LDAP Configuration: Change system configuration to use the LDAP user registry. • Disable LDAP Configuration: Change system configuration to use local user registry based on system internal database.
Store	
Reallocating Unassigned Shards	***Location: Admin Console Utilities Store Reallocating Unassigned Shards*** Reallocating unassigned shards might solve the following situations: 1. An "Error Accessing Store" dialog is displayed after signing in to the system. 2. In the Store page, the status of the cluster is RED with unassigned shards. Use this utility to reallocate unassigned shards to a Store data node. The selected Store node must be a data node (a node of type "D" in the nodes table in the Web Console).

Update Store Allocation Configuration	***Location: Admin Console Utilities Store Store Allocation*** Use this utility to update the application Store size definitions based on the current data file system size.
Cell Environment	
Tune OS Parameters	***Location: Admin Console Utilities Store Tune OS Parameters*** Use this utility to run operating system performance optimization utility.

Dashboards

The dashboards view is the first icon on The Navigation Bar. Clicking on the dashboards icon displays the Navigation Menu and opens the default dashboard in the main window

Graph Functions

Most graph elements in the dashboards supports the drill down feature to speed troubleshooting by narrow to a specific time range around an anomaly.

Top N Graphs

Some dashboards contains graph elements that display a list of top X values.

You can click the drop-down on the top-right side of the header to control how many values the graph will show and your selection will be persisted between sessions.

You can also click on the legend that show a list of values in a top N graph and they will set the value as a filter.

DPOD offers the following categories of dashboards:

Overview Dashboards

The Overview Dashboards include the System Overview, Recent Activity and Activity Distribution dashboards.

These provide you with the most important information you need to grasp the system's health at a glance.

Use these dashboards when you need a bird's eye view of the system or when you need to start your investigation into errors or hold-ups.

Analytics Dashboards

The Analytics Dashboards include the Service Activity, Service per Device, Service Latency and Probes in Use dashboards, which lets you analyze the service health across your system.

These dashboards group transaction information in different aspects, and displays the top five or ten services for each aspect.

Use these dashboards to view the state of services in your system, and quickly identify spikes, problems, errors and behavior anomalies.

Resources Dashboards

The Resources Dashboards include the Device Resources and Service Memory, which let you view the load your infrastructure is under, and the capacity it uses.

Both these dashboards group transaction information in different aspects and display the top five devices or services for each aspect.

Use these dashboards to quickly assert the status and resource consumption across your devices or services.

Security Dashboards

The Security Dashboards include the Expired Certificates, JSON Validation, Security Violations, Non-Secured Connections, Sign and Encryption, SOAP and XML,
and User Login Issues dashboards which provide details of certificates that are either expired or about to expire.

Use theses dashboards to identify security concerns in the system.

Overview Dashboards

DPOD's set of overview dashboards provides the first port-of-call for most actions a user performs inside DPOD. It allows users of different roles to be able to access the information they need to assert the state of the system.
The information provided in these dashboards helps identify anomalies or issues with the system, and lets you drill down to problem areas.

- System Overview
- System Health
- Recent Activity
- Recent Activity (API Connect only)
- Activity Distribution

System Overview

The System Overview dashboard is composed of five widgets that together provide a quick status report about your system components.

System Activity

This widget provides a view of transactions flowing through the system.

The time interval and transaction numbers displayed are filtered according to your filter settings in the Filters Stripe.

Transactions

Successful transactions per second passing through the system.

Transactions Week Before

Successful transactions per second that passed through the system in the same time interval the prior week.

The scale for both the transactions and transactions week before graphs is displayed on the left side of the widget.

Errors

Error transactions per second.

The scale for the error transactions is displayed on the right side of the widget.

Note that the scale for these graphs is different, in order to show meaningful variations in the error graph.

Error Types Explained

The errors displayed here are network or SSL errors. Transactions that are erroneous as a result of the output policy are not reported here, as they are not considered to have ended in an error state.

Device CPU (Top 5)

This widget shows the percentage of CPU used by the five most CPU-bound devices over the time interval.

Device Memory (Top 5)

This widget shows the percentage of Memory used by the five most memory-constrained devices over the time interval.

The Device CPU and Memory widgets may highlight devices that are at or nearing capacity. The information provided could assist in workload re-distribution or adding more devices to the system.

System Errors

The widget displays a table containing all errors logged by the devices (on the default domain only) during the time interval displayed (as controlled by the active filters).

The following information is displayed for each error

Column	Description
Device	The device that reported the error. The device name is a link. Clicking the link will load the Raw Messages Investigate view, with the filters set to display system messages from this device only
Category	The category of the error. The category value within the System Errors widget is always system. Other categories such as network or ws-proxy are available on other views

Severity	The severity of the error. Possible values in the error view are: - error - critic - alert - emerg.
Time	The error’s timestamp
Object Type	The Object Type of the error as reported by a monitored device Log Category
Object Name	The Object Name of the error as reported by monitored device Log Category
Message	The actual error message

The information in this widget can help identify devices that log errors extensively.

System Health

The System Health dashboard provides an overview of all devices health state based on user-defined metrics.

The dashboard is composed of multiple cards, each representing the health of a device, optionally divided into device groups.

In addition, the dashboard displays the DPOD health state based on Internal Health Alerts.

METRICS

- The health of each device is based on several user-defined metrics. For example, the CPU of the device.
- A metric is basically a criteria and a set of thresholds that together define whether the state of the device in that aspect is one of: Good / Waring / Error.
- Metrics are based on the Alerts subsystem of DPOD:
  - The user can define which alerts are part of the System Health by selecting the "System Health Metric" option under [Manage Alert Setup Alerts   Edit Alert].
  - Each alert can be used as a simple alert, as a System Health metric, or both. Using an alert both for alerting and as a System Health metric is recommended, since it makes sure the System Health dashboard will precisely reflect the sent alerts.
- The following System Health metrics are defined by default:
  - Devices CPU Metric
  - Devices Memory Metric
  - Devices Load Metric
  - Devices Fan Metric
  - Devices Temperature Metric
  - Devices Voltage Metric
  - Devices Space Encrypted Metric
  - Devices Space Temp Metric
  - Devices Space Internal Metric
  - System Errors Metric
  - Device Availability Metric - This is an internal metric based on "Device Resources Monitoring" option selected at the device level, that checks whether the device is available or not.

DEVICE HEALTH CALCULATION

- The System Health dashboard calculates the health of each device in the past hour.
- The past hour is divided to 5 parts:
  - Last 5 minutes (may be configured via "System Health Dashboard Sample Time Range (min.)" System Parameter)
  - Previous 10 minutes
  - 3 parts of 15 minutes (the rest of the hour)
- Each part displays a single icon with the health of the device during that period of time:

Icon	Description	Last 5 minutes	Other parts
✓	Good	No errors or warnings found in metric samples	(same)
⚠	Warning	Warnings found in metric samples	(same)
!	Error	Errors found in metric samples OR Warnings count exceeded threshold (see below) OR Warnings damage points exceeded threshold (see below)	(same)
?	Unknown	-	No metric samples found (e.g. DPOD alert subsystem was down) OR The device was unavailable during the entire time period
? + red background color	Critical	No metric samples found (e.g. DPOD alert subsystem was down) OR The device was unavailable in the last "Device Availability Metric" sample	-

- Each device may have a **total warnings threshold** which sets the health of that device to Error in case the number of metrics that are at Warning state exceeds that threshold in a specific time period (see Device Health Settings).
- Each device may also have a **warning damage points threshold** which sets the health of that device to Error in case the summary of the damage points of all metrics that are at Warning state exceeds that threshold in a specific time period (see Device Health Settings).
  - Each System Health metric may be assigned with damage points, which should reflect the severity of that warning.
- For each device, the user can set thresholds and damage points per health metric, which override the default thresholds and damage points defined at the System Health metric level (see Device Health Settings).

DEVICES DISPLAY OPTIONS

- For each device, the user can define whether the device is displayed in the System Health dashboard.
- The user may define device groups:
  - Each device group has a name and a display order of that group
  - Devices are assigned to one or more device groups with a defined display order
  - For example: Production, Non-production

DEVICE HEALTH DASHBOARD

- Clicking a device card in the System Health dashboard opens the Device Health dashboard which displays a detailed view of a specific device health.
- This dashboard displays all metrics that were part of the device health calculation.
- For each metric, all samples are displayed in a chart, which displays each sample values when hovering.
- For analyzing a System Health metric, the user may click "Analyze" when hovering over the metric values. This will take the user to the appropriate dashboard for analyzing the values.
  - Each System Health metric may be assigned with a drill-down dashboard.

Recent Activity

The Recent Activity dashboard provides a bird’s eye view of the system’s most recent activity.

This is perhaps the most suitable view to set to automatically reload every 10 seconds and display on a dedicated monitor in the NOC .

The dashboard is composed of 7 widgets that provide a full picture of the recent activity across the system.
You may filter the information displayed using the Filter Stripe at the top of the window.

Request Size

This widget displays the total size of requests going through the system, alongside a graph showing the distribution of the request size across the time interval displayed.

The triangle at the top right points up or down, adhering to the overall trend of total request size.

Successful Transactions

This widget displays the total count of successful transactions going through, alongside a graph showing the distribution of successful transactions across the time interval displayed.

The triangle at the top right points up or down, corresponding to the overall trend of total transactions throughput.

Errors

This widget displays the total count of errors encountered, alongside a graph showing the distribution of errors across the time interval displayed.
The triangle at the top right points up or down, corresponding to the overall trend of total errors encountered.

System Activity

This is the same widget found in the System Overview Dashboard.

Domain Request Size (Top 5)

This widget shows the 5 domains handling the largest total requests size during the interval displayed.

Note that this widget may show partial or no data if the Domain, Device or Client IP filters are active.

Domain Activity (Top 5)

This widget shows the 5 domains handling the highest number of requests during the interval displayed.

Note that this widget may show partial or no data if the Domain, Device or Client IP filters are active.

Service Errors (Top 5)

This widget shows the 5 services encountering the highest number of errors during the interval displayed.

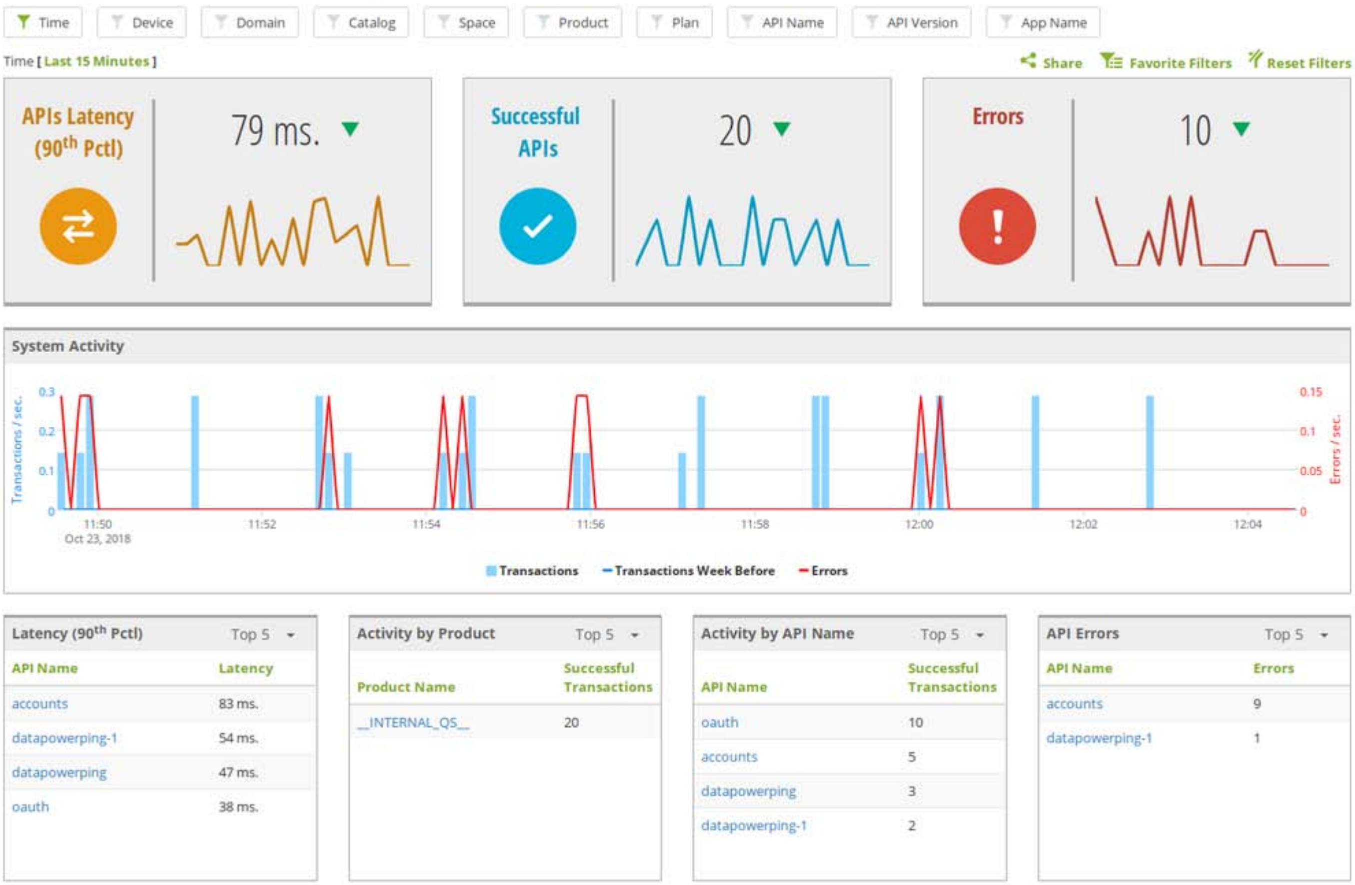
Note that this widget may show partial or no data if the Domain, Device or Client IP filters are active.

Recent Activity (API Connect only)

The API Connect Recent Activity dashboard provides a bird's eye view of the system's most recent activity.

This is perhaps the most suitable view to set to automatically reload every 10 seconds and display on a dedicated monitor in the NOC .

The dashboard is composed of 8 widgets that provide a full picture of the recent activity across the system.
You may filter the information displayed using the Filter Stripe at the top of the window - note that all widget in this page may show partial or no data if the filters are active.



Time [Last 15 Minutes]

APIs Latency (90th Pctl) 79 ms. ▼

Successful APIs 20 ▼

Errors 10 ▼

Latency (90th Pctl) Top 5

API Name	Latency
accounts	83 ms.
datapowerping-1	54 ms.
datapowerping	47 ms.
oauth	38 ms.

Activity by Product Top 5

Product Name	Successful Transactions
__INTERNAL_QS__	20

Activity by API Name Top 5

API Name	Successful Transactions
oauth	10
accounts	5
datapowerping	3
datapowerping-1	2

API Errors Top 5

API Name	Errors
accounts	9
datapowerping-1	1

API Latency (X Percentile)

This widget displays the latency in milliseconds of the X percentile (90th percentile by default) of the APIs going through the system, alongside a graph showing the distribution
of the request size across the time interval displayed.
You can change the percentile shown in system parameters

The number in the middle shows the maximum latency during the time interval.
The triangle at the top right points up or down, adhering to the overall trend of the latency, it may not appear if there was not change in the trend.

Successful APIs

This widget displays the total count of successful APIs going through, alongside a graph showing the distribution
of successful APIs across the time interval displayed.

The triangle at the top right points up or down, corresponding to the overall trend of total transactions throughput, it may not appear if there was not change in the trend.

Errors

This widget displays the total count of errors encountered, alongside a graph showing the distribution of errors across the time interval displayed.
The triangle at the top right points up or down, corresponding to the overall trend of total errors encountered, it may not appear if there was not change in the trend.

System Activity

This is the same widget found in the System Overview Dashboard (showing only API Connect APIs)

Latency (X Percentile, Top 5)

This widget shows the 5 APIs with highest latency during the interval displayed.
You can change the percentile shown in system parameters

Activity by Product (Top 5)

This widget shows the 5 products with highest number of successful transactions during the interval displayed.

Activity by API Name(Top 5)

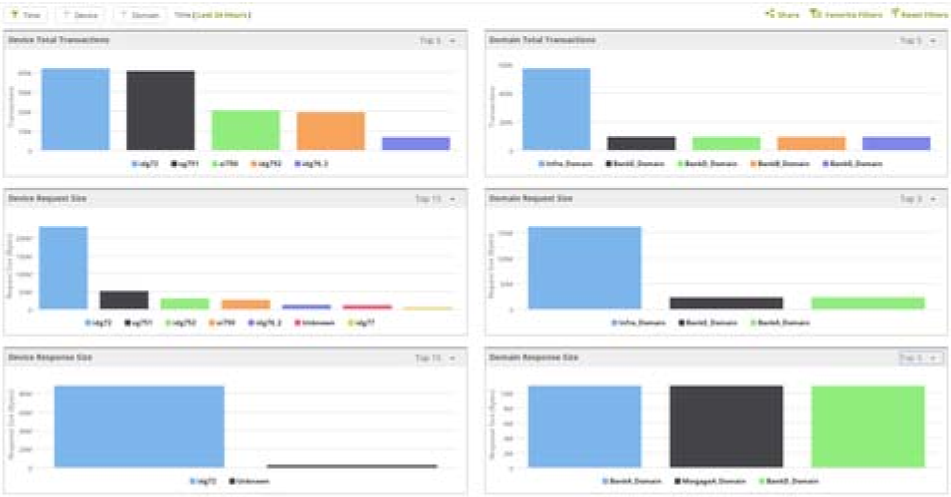
This widget shows the 5 API names with highest number of successful transactions during the interval displayed.

API Errors (Top 5)

This widget shows the 5 APIs encountering the highest number of errors during the interval displayed.

Activity Distribution

The Activity Distribution Dashboard provides insights into the most active devices and domains (adhering to the filter settings you apply) It is composed of 6 graph widgets.



Device Total Transactions (Top 10)

This is a graph of the ten devices serving the highest numbers of transactions in the system.

Domain Total Transactions (Top 10)

This is a graph of the ten domains serving the highest numbers of transactions in the system.

Device Request Size (Top 10)

This is a graph of the ten devices serving the greatest total request size in the system.

Domain Request Size (Top 10)

This is a graph of the ten domains serving the greatest total request size in the system.

Device Response Size (Top 10)

This is a graph of the ten devices serving the greatest total response size in the system.

Domain Response Size (Top 10)

This is a graph of the ten domains serving the greatest total response size in the system.

Analytics Dashboards

DPOD's set of analytics dashboards provides analytics data pertaining to the services and probes in use.

- Service Activity
- Service per Device
- Service Latency
- Service URL Calls
- Service URI Calls
- Restarts
- Active Probes

Service Activity

The service activity dashboard provides two graph widgets that together show activity details of the busiest services in the system (according to the filters applied).

Service Total Transactions (Top 10)

This widget displays the total number of processed transactions across the ten busiest services in the system

Service Transactions (Top 5)

This widget displays the number of transaction per second across the five busiest services in the system.

Service per Device

The Service per Device dashboard provides a break-down of service transactions across devices. It comprises two widgets that show how the transactions are split across devices and services (as filtered by the settings in the Filters Stripe).

Devices Transactions

This widget graphs the transactions per seconds on the devices.

Service Transactions

This widget shows a table of all services, across devices, with their transaction counts.

The following data is available for each service

Column	Description
Device	The device this service is deployed on. Click the device name to load the device in the Transactions view
Service	The service name. Click the service name to load the service in the Transactions view
Transactions Count	Number of transactions for this service, on this device, in the displayed time range

Service Latency

The Service Latency dashboard is composed of 8 widgets that together provide a good overview of how long do the various network tasks take to complete.

By using this dashboard you are able to identify unusually long-running tasks and investigate them further.

All the widgets on this dashboard show only the top 5 services (under the filter restrictions)

Service Elapsed Time (Top 5)

The services taking the most time to complete

DataPower Request Processing (Top 5)

The services taking the most request-processing time.

DataPower Response Processing (Top 5)

The services taking the most response-processing time.

Back-End Processing (Top 5)

The services taking the most back-end processing time.

Back-End Request (Top 5)

The services taking the most back-end request processing time.

Back-End Response (Top 5)

The services taking the most back-end response processing time.

Front-End Request (Top 5)

The services taking the most front-end request processing time.

Front-End Response (Top 5)

The services taking the most front-end response processing time.

Using the information in all the widgets together, you can track tasks throughout their passage in the system.

This lets you analyze trends and bottlenecks that may lead to changes in configuration, setup or code.

Service URL Calls

The service URL calls dashboard displays aggregation of successful transactions without early completion

The transactions are aggregated based on Domain, URL and service URL

> The device name is **not** used for aggregation. Data for identical service names on identical domain names will be aggregated into one row even when running on different devices.
>
> Note that you can still filter the dashboard data by device name(s).

Columns	Description
Domain	The Domain name
URL	Execution URL
Service	Service Name
Avg (ms.)	Average execution time in milliseconds
Max (ms.)	Maximum execution time in milliseconds
Min (ms.)	Minimum execution time in milliseconds
Calls	Number of service calls
X Percentile (90% by default)	The execution time in millisecond of the top X percentile An admin can change the value of X in system parameters
Y Percentile (95% by default)	The execution time in millisecond of the top Y percentile An admin can change the value of Y in system parameters
Z Percentile (99% by default)	The execution time in millisecond of the top Z percentile An admin can change the value of Z in system parameters

Create Alert on Latency

system administrator can create an alert on transactions that took more than a certain time, follow the instructions in the Service URI Calls page

Service URI Calls

The service URI calls dashboard displays aggregation of successful transactions without early completion.

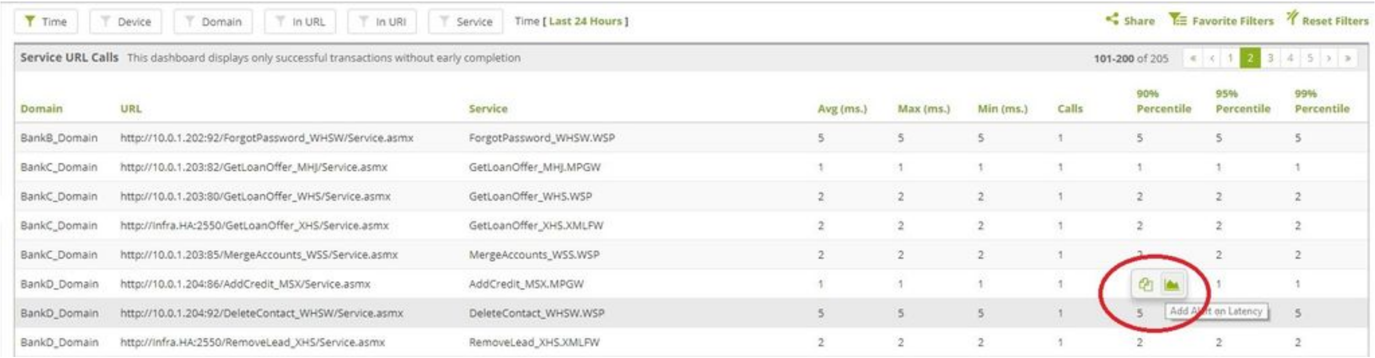
The transactions are aggregated based on Domain, URI and service URI.

> The device name is **not** used for aggregation. Data for identical service names on identical domain names will be aggregated into one row even when running on different devices.
>
> Note that you can still filter the dashboard data by device name(s).

Columns	Description
Domain	The Domain name
URI	Execution URI
Service	Service Name
Avg (ms.)	Average execution time in milliseconds
Max (ms.)	Maximum execution time in milliseconds
Min (ms.)	Minimum execution time in milliseconds
Calls	Number of service calls
X Percentile (90% by default)	The execution time in millisecond of the top X percentile An admin can change the value of X in system parameters
Y Percentile (95% by default)	The execution time in millisecond of the top Y percentile An admin can change the value of Y in system parameters
Z Percentile (99% by default)	The execution time in millisecond of the top Z percentile An admin can change the value of Z in system parameters

Create Alert on Latency

A system administrator can create an alert on transactions that took more than a certain time, hover over the value in the grid, and click "Add alert on latency" in the context menu.



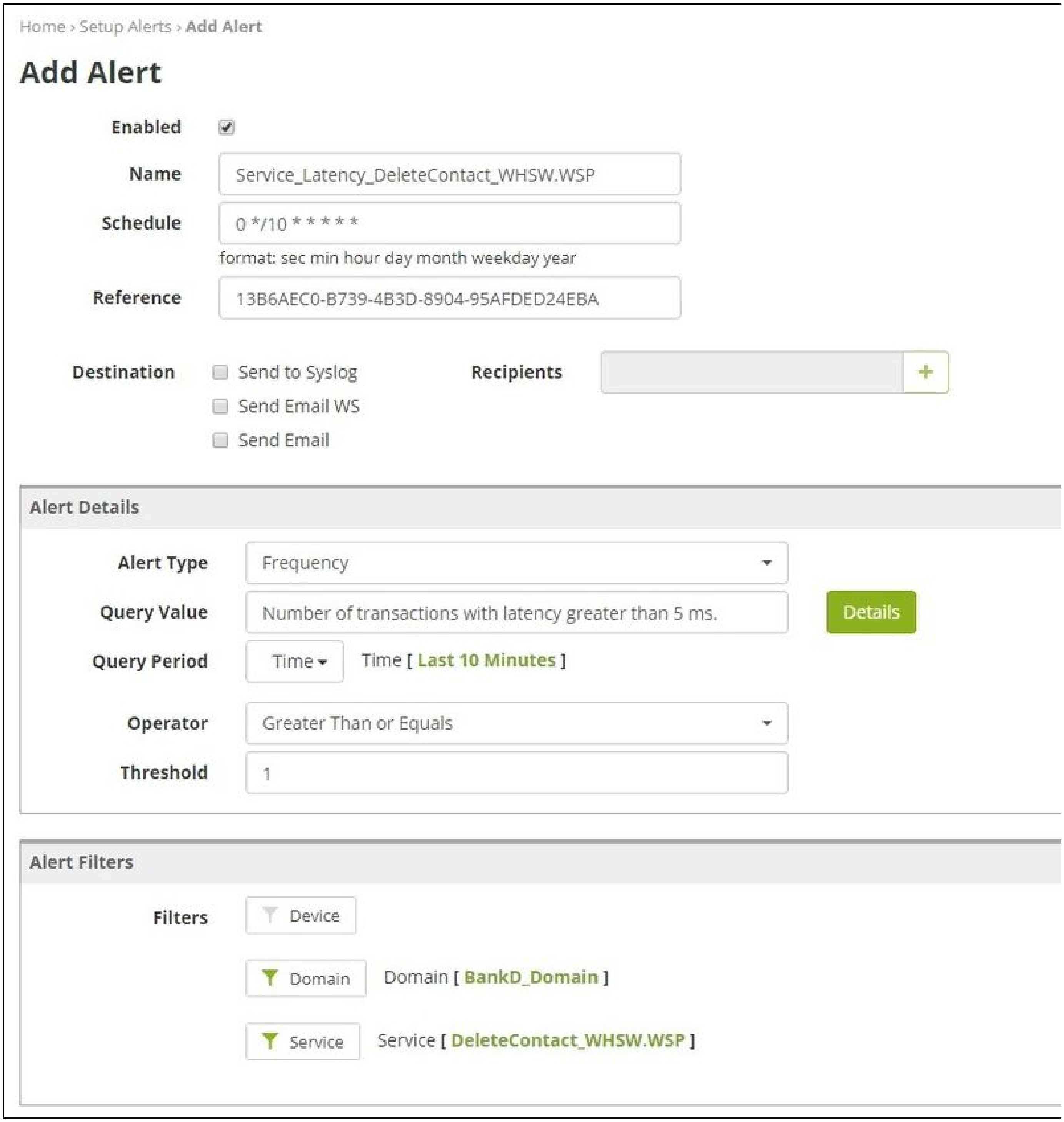
Service URL Calls This dashboard displays only successful transactions without early completion

Domain	URL	Service	Avg (ms.)	Max (ms.)	Min (ms.)	Calls	90% Percentile	95% Percentile	99% Percentile
BankB_Domain	http://10.0.1.202:92/ForgotPassword_WHSW/Service.asmx	ForgotPassword_WHSW.WSP	5	5	5	1	5	5	5
BankC_Domain	http://10.0.1.203:82/GetLoanOffer_MHJ/Service.asmx	GetLoanOffer_MHJ.MPGW	1	1	1	1	1	1	1
BankC_Domain	http://10.0.1.203:80/GetLoanOffer_WHS/Service.asmx	GetLoanOffer_WHS.WSP	2	2	2	1	2	2	2
BankC_Domain	http://infra.HA:2550/GetLoanOffer_XHS/Service.asmx	GetLoanOffer_XHS.XMLFW	2	2	2	1	2	2	2
BankC_Domain	http://10.0.1.203:85/MergeAccounts_WSS/Service.asmx	MergeAccounts_WSS.WSP	2	2	2	1	2	2	2
BankD_Domain	http://10.0.1.204:86/AddCredit_MSX/Service.asmx	AddCredit_MSX.MPGW	1	1	1	1	[illegible]	1	1
BankD_Domain	http://10.0.1.204:92/DeleteContact_WHSW/Service.asmx	DeleteContact_WHSW.WSP	5	5	5	1	5	[illegible]	5
BankD_Domain	http://infra.HA:2550/RemoveLead_XHS/Service.asmx	RemoveLead_XHS.XMLFW	2	2	2	1	2	2	2

The Add Alert page will open, the relevant fields will be automatically filled for you, you will need to set the destination (syslog and/or email recipients)
Click on "Add" to create the alert

Feel free to change any field - specifically, the alert name, schedule and threshold (how many transactions with latency more than X ms will trigger the alert - the default is 1)

> In order to change the alert's latency itself, click on "Details" next to the Query Value, Edit the field "Query (JSON)" and change the number that follows the text "WDPLatency12":{"gte":



Add Alert

Enabled ☑

Name: Service_Latency_DeleteContact_WHSW.WSP

Schedule: 0 */10 * * * * *

format: sec min hour day month weekday year

Reference: 13B6AEC0-B739-4B3D-8904-95AFDED24EBA

Destination: □ Send to Syslog □ Send Email WS □ Send Email

Recipients: +

Alert Details

Alert Type: Frequency

Query Value: Number of transactions with latency greater than 5 ms.

Query Period: Time ▾ Time [Last 10 Minutes]

Operator: Greater Than or Equals

Threshold: 1

Alert Filters

Filters: Device

Domain — Domain [BankD_Domain]

Service — Service [DeleteContact_WHSW.WSP]

Restarts

The restarts dashboard shows a list of domain and device restarts and reloads.

DPOD classifies the restarts into 5 categories:

1. Device Initiated - restarts initiated by the DataPower due to a reason (e.g. low memory)
2. User Initiated - a restart that was initiated by a user via the web interface, CLI, etc.
3. First Boot - the first startup of the device (the restart count is 1)
4. Unexpected - for example, due to a power failure
5. Domain Restart - a user initiated domain restart

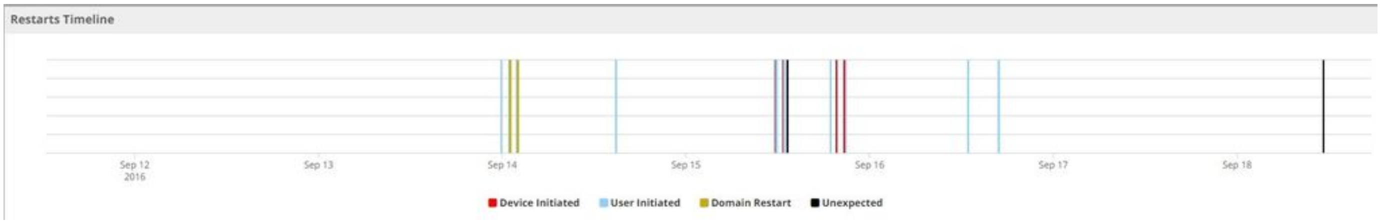
DPOD analyzes the restarts by reading the monitored device's audit logs every 15 minutes, you can change this interval through the Web Console by navigating to ManageSystem ParametersInterval in Seconds to Analyze Audit Logs.

The Restarts Dashboard contains 4 parts:

1. A graph showing the restarts over a timeline
2. The Device memory graph (a device initiated restart is often related to memory issues)
3. Device and domain restarts table
4. Last sample time table

Restarts Timeline

The chart shows all the restarts on a timeline.
Zoom over a specific part of the graph to apply the time period as a filter.
Click on the restart cause (Device Initiated, User Initiated, etc.) in the legend to reload the page with this restart cause as a filter.



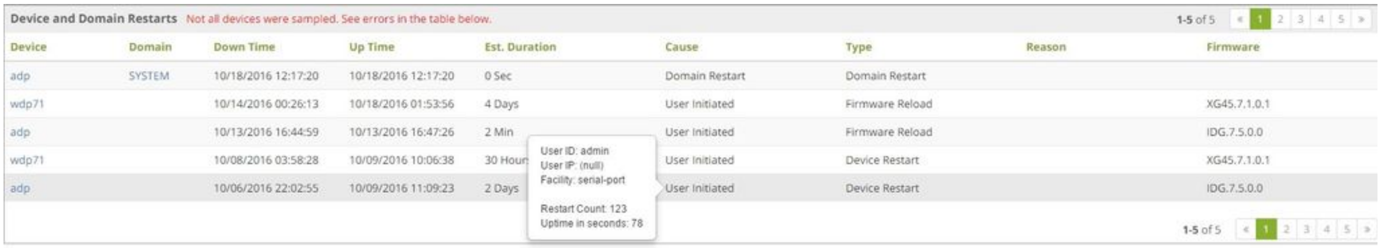
Device and Domain Restarts Table

The table shows all the restarts in a chronological order.

> When one of the devices was not sampled or analyzed, an error message will appear in the table's header alongside the title.
> It may suggest that one of the devices is currently experiencing downtime.
> Check the "Last sampling time" table at the bottom of the page for more information.

Column	Description
Device	The monitored device name
Domain	Populated only for Domain restarts
Down Time	Contains the timestamp of the audit log record that preceded the restart message For "Unexpected Restart" the Down Time figure is an estimation, Since the DataPower logs will not contain any shutdown message, DPOD will try to use the last time it received Resource Monitoring data from the device.
Up Time	Contains the timestamp of the audit log record that signaled that the device was started
Est. Duration	The downtime duration (rounded)
Cause	Device Initiated, User Initiated, Unexpected or Domain Restart. Hover over the cell to get more information about the user who initiated the restart

Type	Either "Firmware Reload" or "Device Restart"
Reason	Populated only for "Device Initiated" restarts
Firmware	The firmware version Hover over the cell to get more information about the IDG version and build information



Device and Domain Restarts Not all devices were sampled. See errors in the table below.

1-5 of 5 « 1 2 3 4 5 »

Device	Domain	Down Time	Up Time	Est. Duration	Cause	Type	Reason	Firmware
adp	SYSTEM	10/18/2016 12:17:20	10/18/2016 12:17:20	0 Sec	Domain Restart	Domain Restart		
wdp71		10/14/2016 00:26:13	10/18/2016 01:53:56	4 Days	User Initiated	Firmware Reload		XG45.7.1.0.1
adp		10/13/2016 16:44:59	10/13/2016 16:47:26	2 Min	User Initiated	Firmware Reload		IDG.7.5.0.0
wdp71		10/08/2016 03:58:28	10/09/2016 10:06:38	30 Hour	User Initiated	Device Restart		XG45.7.1.0.1
adp		10/06/2016 22:02:55	10/09/2016 11:09:23	2 Days	User Initiated	Device Restart		IDG.7.5.0.0

User ID: admin
User IP: (null)
Facility: serial-port

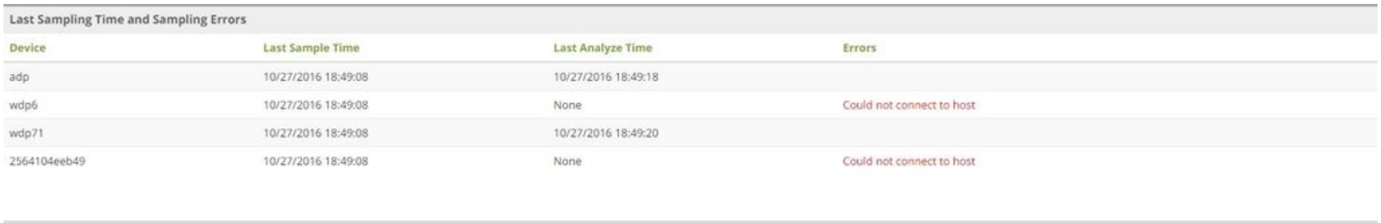
Restart Count: 123
Uptime in seconds: 78

1-5 of 5 « 1 2 3 4 5 »

Last Sampling Time and Sampling Errors Table

This table shows the last time DPOD readi and analyzed the audit logs for each monitored device

Column	Description
Device	The monitored device name
Last Sample Time	The last time DPOD accessed the device audit logs
Last Analyze Time	The last time DPOD analyzed the audit logs
Errors	Lists any errors that occurred, e.g. "Could not connect to host"



Last Sampling Time and Sampling Errors

Device	Last Sample Time	Last Analyze Time	Errors
adp	10/27/2016 18:49:08	10/27/2016 18:49:18	
wdp6	10/27/2016 18:49:08	None	Could not connect to host
wdp71	10/27/2016 18:49:08	10/27/2016 18:49:20	
2564104eeb49	10/27/2016 18:49:08	None	Could not connect to host

Active Probes

The Active Probes dashboard comprises two widgets that provide information about the probes set up in the system.

Policy Rules with Active Probes (Top 5)

This widget shows the 5 services with most probe actions assigned to them.

Policy Rules with Active Probes

This widget shows a table of all services with probes enabled.

Probes, like every other trace mechanism, have significant impact on the monitored device resource consumption. It is therefore important to be able to identify their usage
and monitor their impact on running transactions.

A common action derived from the information provided in the table is to switch a probe off, especially in production environments.

The following data is available in the table:

Column	Description
Service	The service the probe is running on. Click the service name to apply a service filter to the dashboard
Device	The device the service is running on. Click the device name to apply a device filter to the dashboard
Domain	The domain the service is running on. Click the domain name to apply a domain filter to the dashboard
Probes Use	The number of probes used for the service

Analytics Dashboards (API Connect)

- API Activity
- API Latency
- API Versions
- API Policies
- HTTP Res. Codes
- Consumers
- API Availability
- API URL Calls
- API URI Calls

API Activity

The API activity dashboard provides two graph widgets that together show activity details of the busiest APIs in the system (according to the filters applied).

API Total Transactions (Top 15)

This widget displays the total number of processed transactions across the fifteen busiest APIs in the system.

API Transactions (Top 10)

This widget displays the number of transaction per second across the ten busiest APIs in the system.

API Latency

The API latency dashboard provides six graph widgets that together show usage overview of the the slowest/busiest APIs in the system (according to the filters applied).

API Avg Elapsed Time

This widget displays the average elapsed time of transaction per second across the ten slowest APIs in the system.

API Max Elapsed Time

This widget displays the maximum elapsed time of transaction per second across the ten slowest APIs in the system.

API Successful Transactions

This widget displays the number of successful transactions per second across the ten busiest APIs in the system.

API Error Transactions

This widget displays the number of unsuccessful transactions per second across the ten busiest APIs in the system.

API Request Size

This widget displays the average of transactions request size per second across the ten most bandwidth consuming APIs in the system.

API Response Size

This widget displays the average of transactions reponse size per second across the ten most bandwidth consuming APIs in the system.

API Versions

The API versions dashboard provides six graph widgets that together show usage overview of the the slowest/busiest versions of APIs in the system.

API Avg Elapsed Time

This widget displays the average elapsed time of transaction per second across the ten slowest versions of APIs in the system.

API Max Elapsed Time

This widget displays the maximum elapsed time of transaction per second across the ten slowest versions of APIs in the system.

API Successful Transactions

This widget displays the number of successful transactions per second across the ten busiest versions of APIs in the system.

API Error Transactions

This widget displays the number of unsuccessful transactions per second across the ten busiest versions of APIs in the system.

API Request Size

This widget displays the average of transactions request size per second across the ten most bandwidth consuming versions of APIs in the system.

API Response Size

This widget displays the average of transactions reponse size per second across the ten most bandwidth consuming versions of APIs in the system.

API Policies

The API policies dashboard displays aggregation of successful transactions.

The transactions are aggregated based on API name, API version and API policy name.

> The device name is **not** used for aggregation. Data for identical API names, version and policies will be aggregated into one row even when running on different devices, domains, etc...
>
> Note that you can still filter the dashboard data by device name(s).

Columns	Description
API Name	API name
API Version	API version
Policy Name	Activity name in API diagram/assembly
Avg (ms.)	Average execution time in milliseconds
Max (ms.)	Maximum execution time in milliseconds
Min (ms.)	Minimum execution time in milliseconds
Calls	Number of API calls
X Percentile (90% by default)	The execution time in millisecond of the top X percentile
Y Percentile (95% by default)	The execution time in millisecond of the top Y percentile
Z Percentile (99% by default)	The execution time in millisecond of the top Z percentile

An admin can change the percentage of the percentile columns (X,Y,Z) in System Parameters.

HTTP Res. Codes

The HTTP Res. Codes dashboard provides two graph widgets that together shows details about the most common HTTP response codes returned by the API to the calling client.

HTTP Response Codes Count (Top 15)

This widget displays the total number of transactions across the fifteen most common HTTP response codes returned by the API.

API Transactions (Top 10)

This widget displays the number of transaction per second across the the ten most common HTTP response codes returned by the API.

Consumers

The consumers dashboard provides two graph widgets that together show details of the most active API consumers in the system.

Consumer Apps Total Transactions

This widget displays the number of total transactions per consumer application name.

Consumer Apps Transactions

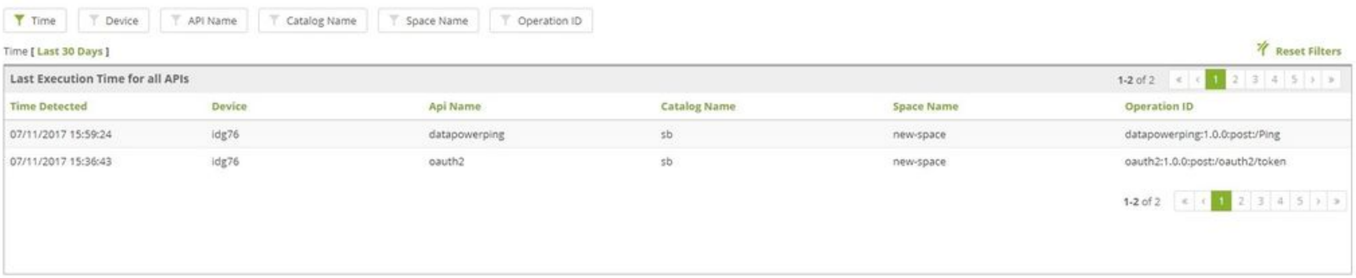
This widget displays the number of transactions per second across consumer applications in the system.

API Availability

This dashboard is only available for the API Connect product view (see product views on how to switch product views)

The dashboard shows the recent execution time for all APIs

> If an API was not executed within the selected time frame, it will not be shown in the dashboard



Time [Last 30 Days]

Last Execution Time for all APIs

Time Detected	Device	Api Name	Catalog Name	Space Name	Operation ID
07/11/2017 15:59:24	idg76	datapowerping	sb	new-space	datapowerping:1.0.0:post:/Ping
07/11/2017 15:36:43	idg76	oauth2	sb	new-space	oauth2:1.0.0:post:/oauth2/token

Column	Description
Time Detected	Last execution time of the API
Device	The DataPower device name
API Name	The API Name
Catalog Name	The API Catalog Name
Space Name	The API Space Name
Operation ID	The invoked operation within the API

API URL Calls

The API URL calls dashboard displays aggregation of successful APIs.

The transactions are aggregated based on URL.

> The device name is **not** used for aggregation. Data for identical URLs will be aggregated into one row even when running on different devices.
>
> Note that you can still filter the dashboard data by device name(s).

Columns	Description
URL	Execution URL
Avg (ms.)	Average execution time in milliseconds
Max (ms.)	Maximum execution time in milliseconds
Min (ms.)	Minimum execution time in milliseconds
Calls	Number of service calls
X Percentile (90% by default)	The execution time in millisecond of the top X percentile An admin can change the value of X in system parameters
Y Percentile (95% by default)	The execution time in millisecond of the top Y percentile An admin can change the value of Y in system parameters
Z Percentile (99% by default)	The execution time in millisecond of the top Z percentile An admin can change the value of Z in system parameters

Create Alert on Latency

system administrator can create an alert on transactions that took more than a certain time, follow the instructions in the Service URI Calls page

API URI Calls

The API URI calls dashboard displays aggregation of successful APIs.

The transactions are aggregated based on URI.

> The device name is **not** used for aggregation. Data for identical URIs will be aggregated into one row even when running on different devices.
>
> Note that you can still filter the dashboard data by device name(s).

Columns	Description
URI	Execution URI
Avg (ms.)	Average execution time in milliseconds
Max (ms.)	Maximum execution time in milliseconds
Min (ms.)	Minimum execution time in milliseconds
Calls	Number of service calls
X Percentile (90% by default)	The execution time in millisecond of the top X percentile An admin can change the value of X in system parameters
Y Percentile (95% by default)	The execution time in millisecond of the top Y percentile An admin can change the value of Y in system parameters
Z Percentile (99% by default)	The execution time in millisecond of the top Z percentile An admin can change the value of Z in system parameters

Create Alert on Latency

system administrator can create an alert on transactions that took more than a certain time, follow the instructions in the Service URI Calls page

Resources Dashboards

DPOD's set of resources dashboards provides an overview of device and service resource consumption throughout the system.

- Device Resources
- Service Memory
- Gateway MQ Overview

Device Resources

The Device Resources dashboard is composed of 9 widgets that provide detailed information about your devices health and resource consumption.

The display may be filtered to display information over specific interval and only include some devices.

The information displayed by these widgets may highlight devices that are at or nearing capacity. It can therefore assist in workload redistribution or aid making the decision to add more devices to the system.

Some of the widgets provide physical health information about the machines in your system. The information presented by them can be used to identify imminent failures or degrading hardware capabilities.

Device CPU (Top 5)

This widget shows the percentage of CPU used by the five most CPU-bound devices over the time interval.

Device Memory (Top 5)

This widget shows the percentage of Memory used by the five most memory-constrained devices over the time interval.

Device Load (Top 5)

This widget shows the system usage load for devices over a time interval. (See load definition)

Device Encrypted FileSystem (Top 5)

This widget shows the percentage of the encrypted file system used by those devices that use it most.

Device Temporary FileSystem (Top 5)

This widget shows the percentage of the temporary file system used by those devices that use it most.

Device Internal FileSystem (Top 5)

This widget shows the percentage of the internal file system used by those devices that use it most.

Device Fan Health (Top 5)

This widget shows the percentage of operating fans of all fans installed on selected devices. For example: When 8 of the 10 fans installed are working the Fan Health value will be reported as 80%.

The information in this widget applies to physical appliance only.

Device Temperature (Top 5)

This widget shows the percentage of temperature sensors that report within a valid metric range of all temperature sensors installed on each selected device. For example: When 8 of the 10 sensors installed report within the valid range, the Device Temperature value will be reported as 80%.

The information in this widget applies to physical appliance only.

Device Voltage Health (Top 5)

This widget shows the percentage of voltage sensors that report within a valid metric range of all voltage sensors installed on each selected device. For example: When 8 of the 10 sensors installed report within the valid range, the Voltage Health value will be reported as 80%.

The information in this widget applies to physical appliance only.

Ethernet Interfaces Rx / TX (MB) (Top 5)

This widget shows the traffic in MB that was sent/received by all Ethernet interfaces on the device.

Ethernet Interfaces Rx / TX Errors (Top 5)

This widget shows the number of errors (send/receive) for all Ethernet interfaces on the device.

Ethernet Interfaces Rx / TX Drops (Top 5)

This widget shows the number of send/receive drops for all Ethernet interfaces on the device.

Service Memory

The Service Memory dashboard contains a single widget.

Service Memory (Top 5)

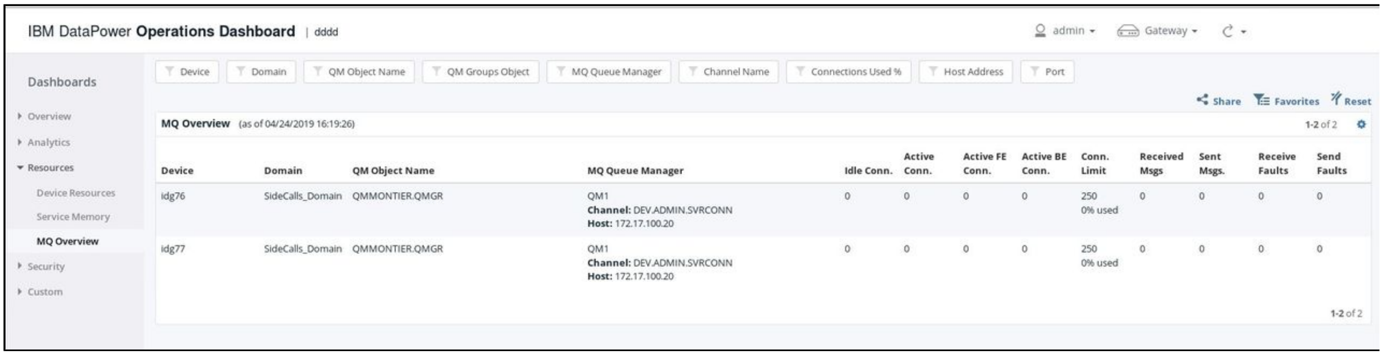
This widget provides information about the 5 most memory-consuming services in the system.

The information is aggregated from periodical samples and do not therefore provide a real-time view of the system.

Gateway MQ Overview

The gateway MQ Overview dashboard shows a summary of MQ objects configuration and statistics
The data is sampled at certain intervals, admin users can change this interval by changing the system parameter Interval in Seconds to Sample Gateway MQ Objects Stats

The latest sample time is shown on the grid's title.



MQ Overview (as of 04/24/2019 16:19:26)

Device	Domain	QM Object Name	MQ Queue Manager	Idle Conn.	Active Conn.	Active FE Conn.	Active BE Conn.	Conn. Limit	Received Msgs	Sent Msgs.	Receive Faults	Send Faults
idg76	SideCalls_Domain	QMMONTIER.QMGR	QM1 **Channel:** DEV.ADMIN.SVRCONN **Host:** 172.17.100.20	0	0	0	0	250 0% used	0	0	0	0
idg77	SideCalls_Domain	QMMONTIER.QMGR	QM1 **Channel:** DEV.ADMIN.SVRCONN **Host:** 172.17.100.20	0	0	0	0	250 0% used	0	0	0	0

1-2 of 2

Column	Description
Device	The gateway's name
Domain	The domain name
QM Object Name	The "IBM MQ Queue Manager" Object name on the gateway If the object belongs to one or more groups (gateway object "IBM MQ Queue Manager Group") - the names of the groups will appear below the object name
MQ Queue Manager	The information is split to three lines: The MQ Queue Manager name The MQ Queue Manager channel name The MQ Queue Manager host name
Idle Connections	Total number of idle TCP connections established by this IBM MQ queue manager.
Active Connections	Total number of active TCP connections established by this IBM MQ queue manager.
Active FE Connections	Number of active front-end TCP connections established by this IBM MQ queue manager.
Active BE Connections	Number of active back-end TCP connections established by this IBM MQ queue manager.
Connections Limit	Total number of open TCP connections to allow by this IBM MQ queue manager. The second line shows the percent of used connections (100 x Active Connections / connections limit)
Received Msgs	Number of messages received by this IBM MQ queue manager.
Sent Msgs.	Number of messages sent by this IBM MQ queue manager.
Receive Faults	Number of messages received with faults.
Send Faults	Number of messages sent with faults.

Security Dashboards

DPOD's set of security dashboards provide insights into security-related events. Using the information in these dashboards can aid in identifying security risks across the system.

- Expired Certificates
- JSON Validation
- Security Violations
- Non-Secured Connections
- Sign and Encryption
- SOAP and XML
- User Login Issues

Expired Certificates

The dashboard shows information on Certificates Expiration.

The certificate monitor scans **only** certificate files that are configured using DataPower’s “crypto Certificate” object.

If you only uploaded certificate files but did not configure a corresponding Crypto Object, the certificate will not be sampled by the certificate monitor.

Please note the certificate monitor is scheduled to run on an interval defined in System Parameters .

This dashboard contains two widgets.

Expired Certificates

This widget lists the expired certificates encountered in the system. The table lists the following details for each expired certificate:

Column	Description
Device	The device an expired certificate is installed on. Clicking on the device name adds a device filter to the display
Time	Timestamp of the expiry message log entry
Details	The expired certificate name and the domain it is installed on

Certificates About to Expire

This widget provides details of certificates expiring within a pre-defined number of days. The display pertains only to certificates located on a file system of a monitored device.
The number of days can be configured by DPOD's admin using the System Parameters.

Note: Certificate Monitoring has to be enabled by an administrator

For each imminently expiring certificate the table lists the following information:

Column	Description
Device	The device this certificate is installed on. Clicking on the device name adds a device filter to the display
Time	Timestamp of the warning of future expiry message log entry
Details	The certificate name and the domain it is installed on

JSON Validation

The JSON validation violations dashboard presents information pertaining to JSON validation events encountered in the system.

While Payload validation failures may occur under normal flow, it can also indicate payload-based attacks.

The data is displayed in a table. For each validation violation, the table details the following information:

Column	Description
Device	The device that encountered the security violation. Clicking on the device name applies a device-filter.
Time	Violation’s Timestamp
Object Name	The violation’ object name
Object Type	The violation’s object type
Category	The violation’s category
Severity	The violation’s severity
Message Code	The message code associated with the violation
Message	The message associated with the violation

Security Violations

The security violations dashboards presents information pertaining to security policy violations encountered in the system. The data is displayed in a table with the following information:

Column	Description
Device	The device that encountered the security violation. Clicking on the device name applies a device-filter.
Time	Violation’s Timestamp
Object Name	The violation’ object name
Object Type	The violation’s object type
Category	The violation’s category
Severity	The violation’s severity
Message Code	The message code associated with the violation
Message	The message associated with the violation

Non-Secured Connections

This dashboard provides details of SOAP and XML errors that occurred throughout the system. The data is displayed in a table with the following information:

Column	Description
Device	The device that encountered the error. Clicking on the device name applies a device-filter.
Time	Error Timestamp
Object Name	The error’s object name
Object Type	The error’s object type
Category	The error’s category
Severity	The error’s severity
Message Code	The message code associated with the error
Message	The message associated with the error

Sign and Encryption

This dashboard provides details of failed encryption,decryption, signing and verifying operation errors that occurred throughout the system.

A failed to verify a signed request may occur as a result of request tampering.

The data is displayed in a table with the following information:

Column	Description
Device	The device that encountered the error. Clicking on the device name applies a device-filter.
Time	Error Timestamp
Object Name	The error’s object name
Object Type	The error’s object type
Category	The error’s category
Severity	The error’s severity
Message Code	The message code associated with the error
Message	The message associated with the error

SOAP and XML

This dashboard provides details of SOAP and XML errors that occurred throughout the system. The data is displayed in a table with the following information:

Column	Description
Device	The device that encountered the error. Clicking on the device name applies a device-filter.
Time	Error Timestamp
Object Name	The error’s object name
Object Type	The error’s object type
Category	The error’s category
Severity	The error’s severity
Message Code	The message code associated with the error
Message	The message associated with the error

User Login Issues

This dashboard provides information about erroneous user login events, that may be considered as an attack on the system,
The following details are provided for each event:

Column	Description
Device	The device that encountered the event. Clicking on the device name applies a device-filter
Time	Event Timestamp
Object Name	The username for which the event happened
Object Type	Will always display 'user'
Category	Will always display 'auth
Severity	The event’s severity
Message Code	The message code associated with the event
Message	The message associated with the event

Custom Dashboards

Admins can design custom dashboards containing DPOD widgets (see Dashboards Editor).

Custom dashboards that are enabled, are available to all users from the Dashboards menu.

Investigate

Clicking on the Investigate icon in the navigation bar opens the investigation view in the main window.
You may also get to this view directly from some dashboards by using table links.

For example, in the Service per Device dashboard, clicking a device name in the **Services Successful Transaction** widget will load the **Transactions** widget under the Investigation view.

The investigation view is split into four sub-views:

Transactions

Raw Messages (for admins or users with appropriate permissions)

Extended Transactions

Payload Capture (for admins or users with appropriate permissions)

Policy Variables Capture (API-C only, for admins or users with appropriate permissions)

Raw Messages

The raw messages widget displays a list of the raw messages sent from log targets of monitored devices across the system, filtered according to the active filter settings.
Any message captured by the system is eligible to be displayed here, regardles of whether or not it culminated in a transaction.

Example

A message contatining an invalid SSL request is invalid, or sent to a URL that DataPower does not process, will not be treated as a transaction by the system. These messages are only classified as requests, that are displayed inside the Raw Messages widget.

The following information is available for each raw message

Column	Description
Device	The Device the message ran on. Clicking on the device's name applies a device filter to the list.
Domain	The Domain the message ran on. Clicking on the domain's name applies a domain filter to the list.
Category	Message Category. This is the message's category. These are either built-in or set by the user.
Severity	Severity of the message. Ordered from low to high: • Debug • Info • Notice • Error
Time	Time the message was logged
Direction	The message's direction. This may be: • Request • Response • Error (if the message is an error) • Empty (if it is a system message).
Object Type	The object type associated with this message
Object Name	The object name associated with this message
Transaction ID	The transaction id of the transaction encompassing this raw message. Clicking the transaction id link will display a Single Transaction view for this transaction (or API Connect Single Transaction page, depends on the product view)
Client IP	The Client IP this message originated from. This may be the actual client, or a load balancer.
Message Code	The syslog message code
Message	The actual message logged
Gl. Trans. ID **	The Global Transaction ID
B2B Msg. ID **	The B2B Message ID (if applicable)
B2B From Partner ID **	The B2B From Partner ID (if applicable)
B2B To Partner ID **	The B2B To Partner ID (if applicable)
B2B From Partner Profile **	The B2B From Partner Profile (if applicable)
B2B To Partner Profile **	The B2B To Partner Profile (if applicable)

** This field is not displayed by default, an admin can select which fields are shown by changing the "IDG Raw Message Page Columns" parameters from the system parameters page.

Transactions Views

Product Views allows user to get information about a transaction with its relevant data and terms related to the chosen product.

- DataPower Transactions
- API Connect Transactions

DataPower Transactions

This is the default view when you click to open the Investigate process. It provides details of the transactions in the system, according to the filters set.

Filters

See Available Filters for a complete list of filters.

Transactions Grid

The following information is available for each transaction:

Column	Description
Service Name	The service the running the transaction. Clicking the service name link applies a service filter to the results, showing only transactions across this service
Operation	The operation type of this transaction (may show the Request URI for Multi-Protocol Gateway services)
Time	The time this transaction was logged
Device	The device this transaction ran on. Clicking the device name link applies a device filter to the results, showing only transactions that ran on this device.
Domain	The domain this transaction ran in
Status	The status of the transaction. This may be either OK, ERROR or INPROCESS
Trans Id	This is the monitored device's transaction id. Clicking the Transaction id link loads the Single Transaction details view
Client IP	The client originating the transaction. This can sometimes be the IP of the load balancer.
Elapsed (ms)	The elapsed time of the transaction in milliseconds
Payload	When WS-M recording is on, this column will contain the payload of the transaction.

Note

IN PROCESS transactions may or may not have completed OK. INPROCESS signifies that DPOD has not found an ‘End transaction’ message in the log for this transaction.

DATAPOWER SINGLE TRANSACTION

When you click a transaction’s id in the transactions widget, DPOD loads the full details of the transaction into the information window.

This view provides a plethora of information about the single transaction in the following widgets.

Transaction Widget

The widget at the top left of the information window displays the transaction’s time, status, device, domain, service, operation and Client IP.

This information is identical to the information displayed for the transaction in the DataPower Transactions table.

Transaction Analysis Widget

The widget at the top right provides analysis of the transaction in four aspects:
Error analysis

(For transactions in Error status only).

The errors displayed are either network or SSL errors. Transactions that are erroneous as a result of the output policy are not reported here.

If the error is common, DPOD provides a description alongside the error. This is especially useful in situations where the raw logs are hidden on account of security policies, and cannot be viewed by the user.

DPOD Administrators can also add error analysis descriptions.
Probe Enabled Indicator

If a DataPower probe was enabled during the run of this transaction, an indication will appear ("A probe was enabled for this transaction")
Service Configuration Changes Indicator

If service configuration changes occurred over the last 4 hours/day/week/month, an indication will appear with the number of configuration changes.

Click to drill down into the Service Configuration Changes page. From there, you can view the service configuration changes audit information.
Elapsed Time

A breakdown of the transaction’s elapsed time between network, monitored device and Service Provider.
This analysis lets you view latency data pertaining to the transaction, and potentially identify network congestion or issues.

This data is only available for successful transactions.
Payload Size

Displays the request and response size.
This data is only available since IDG firmware 7.6.0.8 and 7.7.1.2 for transactions of traditional IDG services.
Memory

Memory consumption graphs for the request and response parts of the transaction, across the transaction lifetime and state changes.

The memory graph is designed to display the differences in memory consumption between processing policy actions in a processing rule.

The purpose of this graph is to assist the user in troubleshooting high memory consumption by one or more processing actions (for example when using an inefficient XSLT).

The graph is built using the DataPower “memory-report” records.

In some cases the memory used value reported at the beginning of a transaction is higher than the values following, leading to a negative value in the report.

To investigate the service’s total memory usage navigate to Dashboards   Resources Service Memory.

The memory graph displays the differences in memory usage values in KB.

Raw Messages Tab

This widget lists the raw messages that make up the single transaction viewed (up to 2000 messages).

Tracking the raw messages making up transactions in error may provide insights into the causes of failures.

Tracking the raw messages making up successful transactions may provide insights into slow components or unnecessary steps.

The information is displayed in a table.

Column	Description
Category	The message’s category
Severity	The message’s severity
Time	The message’s timestamp
Direction	The message’s direction. This may be: • Request • Response • Error (if message is an error) • Empty (if it is a system message)
Object Type	The object type associated with this message
Object Name	The object name associated with this message
Client IP	The Client IP this message originated from. This may be the actual client, or a load balancer.
Message Code	The message’s code
Message	The actual message logged.

Payload Tab

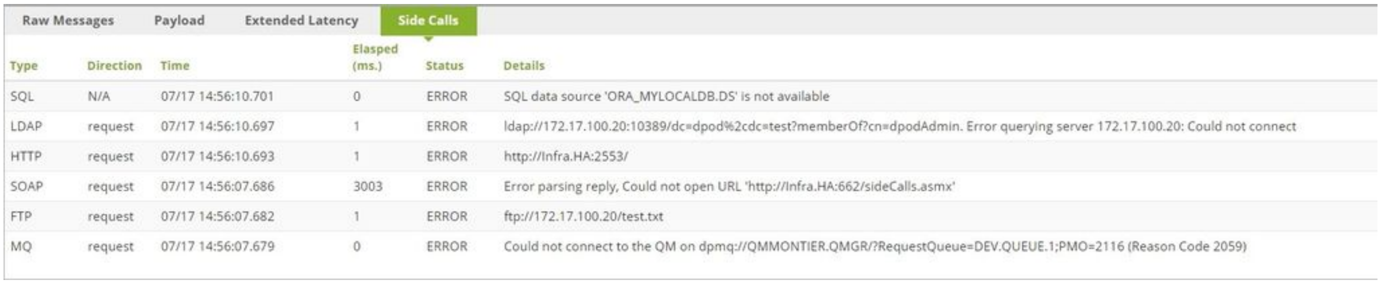
When WS-M recording is switched on, the Payload pane of the table will contain payload information for the messages displayed.
The payload is shown for both the front end and the back end, for both the request and response phases.

Extended Latency Tab

Detailed latency information for both the request and response phases.

Side Calls Tab

The side calls tab shows calls made by the DataPower to external resources during the transaction, such as SQL calls, LDAP, HTTP requests, SOAP requests, FTP calls, MQ calls, etc.



Type	Direction	Time	Elasped (ms.)	Status	Details
SQL	N/A	07/17 14:56:10.701	0	ERROR	SQL data source 'ORA_MYLOCALDB.DS' is not available
LDAP	request	07/17 14:56:10.697	1	ERROR	ldap://172.17.100.20:10389/dc=dpod%2cdc=test?memberOf?cn=dpodAdmin. Error querying server 172.17.100.20: Could not connect
HTTP	request	07/17 14:56:10.693	1	ERROR	http://Infra.HA:2553/
SOAP	request	07/17 14:56:07.686	3003	ERROR	Error parsing reply, Could not open URL 'http://Infra.HA:662/sideCalls.asmx'
FTP	request	07/17 14:56:07.682	1	ERROR	ftp://172.17.100.20/test.txt
MQ	request	07/17 14:56:07.679	0	ERROR	Could not connect to the QM on dpmq://QMMONTIER.QMGR/?RequestQueue=DEV.QUEUE.1;PMO=2116 (Reason Code 2059)

Column	Description
Type	The call type - such as SQL, LDAP, etc.
Direction	request or response
Time	When the call was made
Elapsed (ms.)	Elapsed time of the call in milliseconds
Status	Whether the call was successful or not
Details	Additional details about the call, such as the SQL statement, HTTP request URL, etc

API Connect Transactions

This is the default view when you click to open the Investigate process. It provides details of the transactions in the system, according to the filters set.

Filters

The filters screen the data that is passed at the beginning of the API execution except OAuth, Latency, Response codes and Error messages which are collected at the end of the transaction.
If the API did not finish, the OAuth, Latency, Response codes and Error message will not be collected and will not be displayed in the grid.
See Available Filters for a complete list of filters for the API Connect view.

Most common filters are visible by default. Press " show more ▾ " link to view additional filters.

Transactions Grid

The following information is available for each transaction:

Time	The time this transaction was logged
Device	The device this transaction ran on. Clicking the device name link applies a device filter to the results, showing only transactions that ran on this device.
Catalog/Space	The API catalog name and API space name separated by a slash character (i.e. my-catalog/my-space).
Product	The product name that was consumed by the API call.
Plan	The name of the plan that was used during the API call.
API	The API Name and API Version separated by a dash character (i.e. api-name - 1.0.0).
App Name	The name of the consumer application that made the API call.
URI	The last part of URL which identifies the API invoked by the client.
Status	The status of the transaction. This may be either OK or ERROR.
Trans. ID	The monitored device's transaction ID. Clicking the transaction ID link loads the Single Transaction details view.
Client IP	The IP address of the client originating the transaction. This can sometimes be the IP of the load balancer.
Gl. Trans. ID	The global transaction ID.
Elapsed (ms)	The total elapsed time of the transaction in milliseconds.
Payload	When payload capture is on, this column will contain an icon that indicates the payload is available for this transaction.

API CONNECT SINGLE TRANSACTION

When you click a transaction’s ID in the transactions list, DPOD loads the full details of the transaction into the information window.

This view provides a plethora of information about the single transaction in the following widgets.

Transaction Widget

The widget at the top of the window displays various details about the transaction, sc time, status, device, domain, service, operation and Client IP.

This information is identical to the information displayed for the transaction in the Transactions table.

Transaction Analysis Widget

Error analysis

(For transactions in Error status only).

These are network or SSL errors. Transactions that are erroneous as a result of the output policy are not reported here.

If the error is common, DPOD will provide a description of the error here. This is especially useful in situations where the raw logs are hidden on account of security policies, and cannot be viewed by the user.

DPOD Administrators can also add error analysis descriptions.

Elapsed Time

A breakdown of the transaction’s elapsed time between network, monitored device and Service Provider.
This analysis lets you view latency data pertaining to the transaction, and potentially identify network congestion or issues.

This data is only available for successful transactions.

Payload Size

Displays the request and response size.

Memory

Memory consumption graphs for the request and response parts of the transaction, across the transaction lifetime and state changes.

The memory graph is designed to display the differential memory consumption between processing policy actions in a processing rule.

The purpose is to assist the user in troubleshooting high memory consumption by one or more processing actions (for example when using inefficient XSLT).

The graph is built based on the DataPower “memory-report” records.

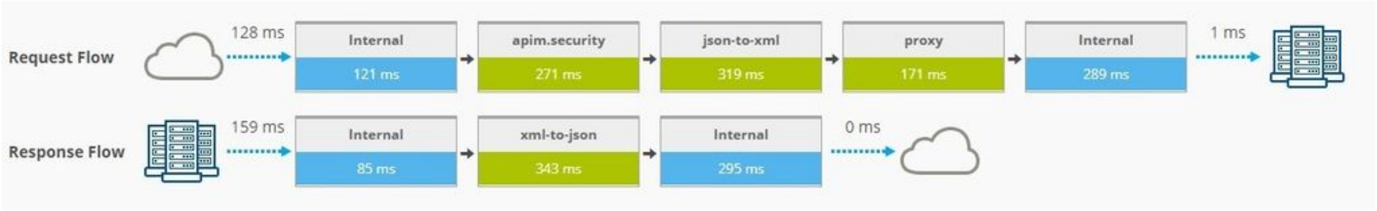
In some cases the memory value reported at the beginning of a transaction is higher than the following memory report leading to a negative value.

To investigate the service’s total memory usage please navigate to Dashboards -> Resources -> Service Memory.

The memory graph display the differential memory value in KB.

Policy Graph

Green nodes represent user policies and their latency, hover over the latency node to view the policy type.
Blue nodes represent the API Framework latency.
Click on a user policy to open the Policy Details Window (more details later on this page)



Raw Messages Tab

The raw messages tab is identical to the raw messages tab in the DataPower transaction page

Payload Tab

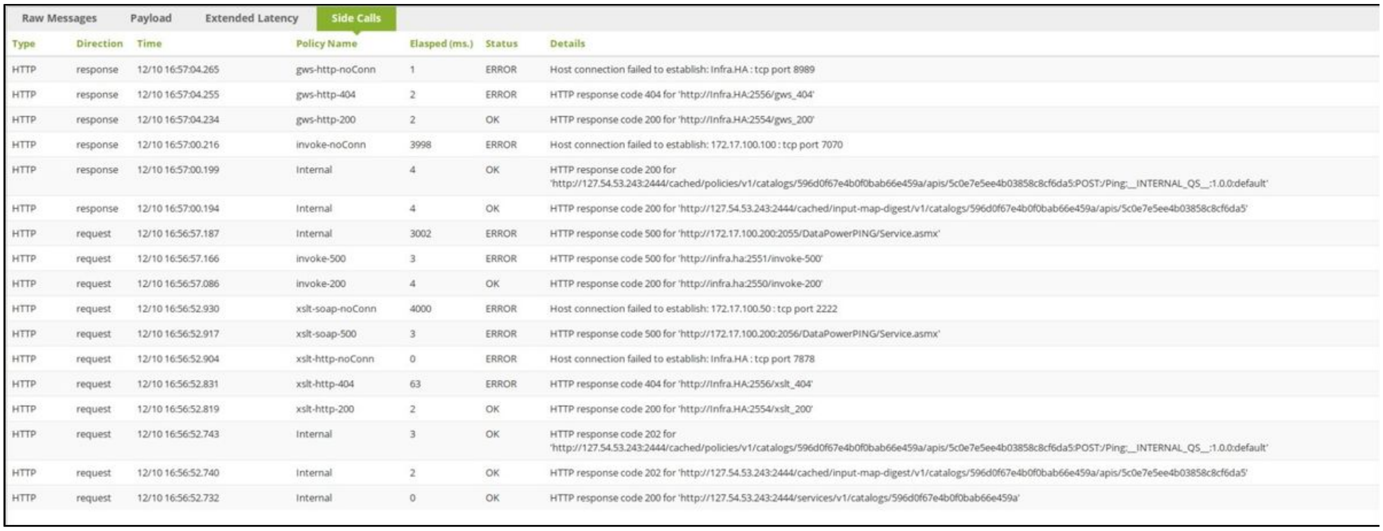
The payload tab is identical to the payload tab in the DataPower transaction page

Extended Latency Tab

The extended latency tab is identical to the extended latency tab in the DataPower transaction page

Side Calls

The side calls tab shows both API-C internal side calls (such as calls to API-C Analytics) and side calls that were made by user policies.

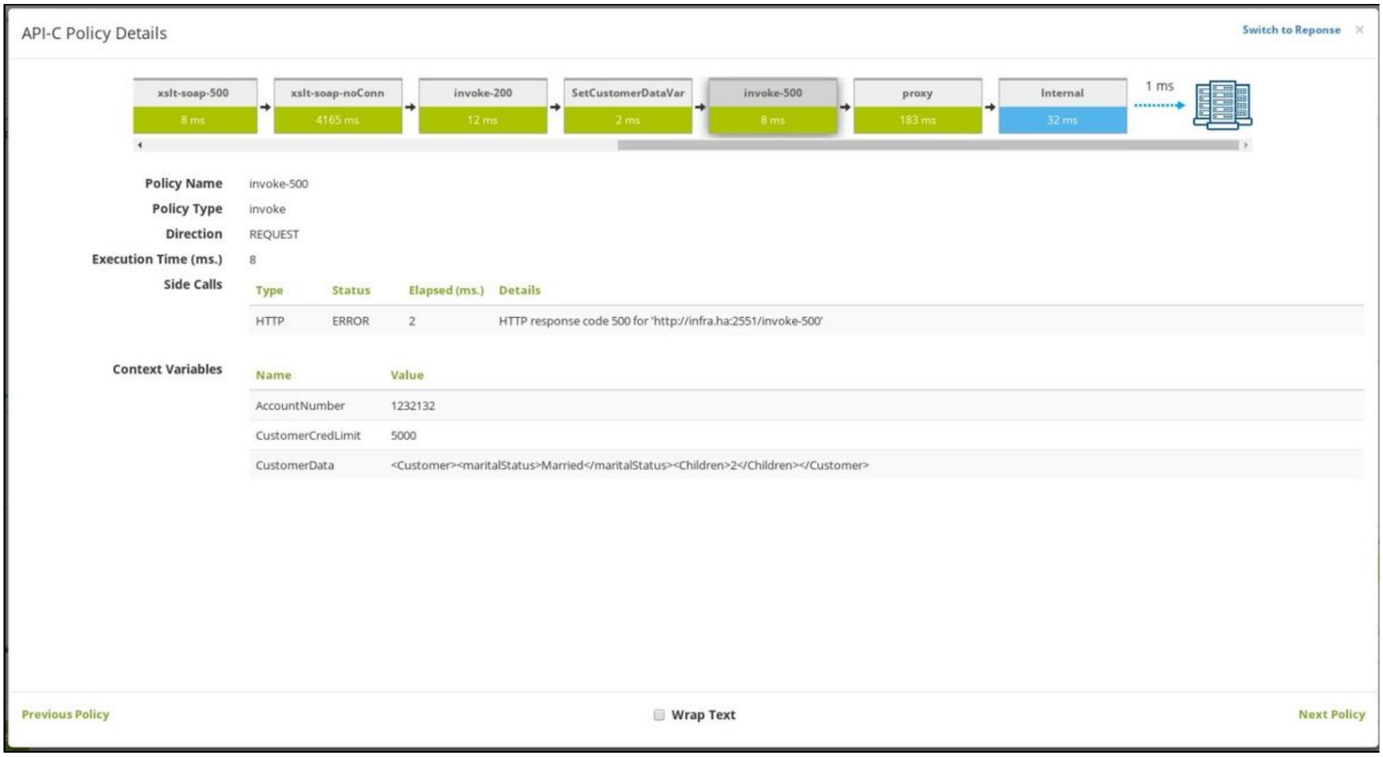


Type	Direction	Time	Policy Name	Elasped (ms.)	Status	Details
HTTP	response	12/10 16:57:04.265	gws-http-noConn	1	ERROR	Host connection failed to establish: Infra.HA : tcp port 8989
HTTP	response	12/10 16:57:04.255	gws-http-404	2	ERROR	HTTP response code 404 for 'http://Infra.HA:2556/gws_404'
HTTP	response	12/10 16:57:04.234	gws-http-200	2	OK	HTTP response code 200 for 'http://Infra.HA:2554/gws_200'
HTTP	response	12/10 16:57:00.216	invoke-noConn	3998	ERROR	Host connection failed to establish: 172.17.100.100 : tcp port 7070
HTTP	response	12/10 16:57:00.199	Internal	4	OK	HTTP response code 200 for 'http://127.54.53.243:2444/cached/policies/v1/catalogs/596d0f67e4b0f0bab66e459a/apis/5c0e7e5ee4b03858c8cf6da5:POST:/Ping:__INTERNAL_QS__:1.0.0:default'
HTTP	response	12/10 16:57:00.194	Internal	4	OK	HTTP response code 200 for 'http://127.54.53.243:2444/cached/input-map-digest/v1/catalogs/596d0f67e4b0f0bab66e459a/apis/5c0e7e5ee4b03858c8cf6da5'
HTTP	request	12/10 16:56:57.187	Internal	3002	ERROR	HTTP response code 500 for 'http://172.17.100.200:2055/DataPowerPING/Service.asmx'
HTTP	request	12/10 16:56:57.166	invoke-500	3	ERROR	HTTP response code 500 for 'http://infra.ha:2551/invoke-500'
HTTP	request	12/10 16:56:57.086	invoke-200	4	OK	HTTP response code 200 for 'http://infra.ha:2550/invoke-200'
HTTP	request	12/10 16:56:52.930	xslt-soap-noConn	4000	ERROR	Host connection failed to establish: 172.17.100.50 : tcp port 2222
HTTP	request	12/10 16:56:52.917	xslt-soap-500	3	ERROR	HTTP response code 500 for 'http://172.17.100.200:2056/DataPowerPING/Service.asmx'
HTTP	request	12/10 16:56:52.904	xslt-http-noConn	0	ERROR	Host connection failed to establish: Infra.HA : tcp port 7878
HTTP	request	12/10 16:56:52.831	xslt-http-404	63	ERROR	HTTP response code 404 for 'http://Infra.HA:2556/xslt_404'
HTTP	request	12/10 16:56:52.819	xslt-http-200	2	OK	HTTP response code 200 for 'http://Infra.HA:2554/xslt_200'
HTTP	request	12/10 16:56:52.743	Internal	3	OK	HTTP response code 202 for 'http://127.54.53.243:2444/cached/policies/v1/catalogs/596d0f67e4b0f0bab66e459a/apis/5c0e7e5ee4b03858c8cf6da5:POST:/Ping:__INTERNAL_QS__:1.0.0:default'
HTTP	request	12/10 16:56:52.740	Internal	2	OK	HTTP response code 202 for 'http://127.54.53.243:2444/cached/input-map-digest/v1/catalogs/596d0f67e4b0f0bab66e459a/apis/5c0e7e5ee4b03858c8cf6da5'
HTTP	request	12/10 16:56:52.732	Internal	0	OK	HTTP response code 200 for 'http://127.54.53.243:2444/services/v1/catalogs/596d0f67e4b0f0bab66e459a'

Policy Details Window

The top part of the window shows the policy graph, you can focus on any user policy by clicking it, click on "Switch to Response/Request" to change the displayed direction.
The middle part shows general details about the policy, such as the policy name, type and direction and the execution time in ms.
The lower part shows a list of side calls made by this policy. and a list of context variables and their values (if a policy variables capture was active during the execution of this transaction)
If a policy variables capture was active, but no data is showing in the "Context variables" table - wait a few seconds and refresh the page, it may take up to 2 minutes for the data to appear.

Keyboard shortcuts -
Left or Right arrows - Previous / Next policy
Enter - Switch between requests and responses.
Space - Wrap the policy variables values text.
Escape - close the window.



Policy Name	invoke-500
Policy Type	invoke
Direction	REQUEST
Execution Time (ms.)	8

Side Calls

Type	Status	Elapsed (ms.)	Details
HTTP	ERROR	2	HTTP response code 500 for 'http://infra.ha:2551/invoke-500'

Context Variables

Name	Value
AccountNumber	1232132
CustomerCredLimit	5000
CustomerData	<Customer><maritalStatus>Married</maritalStatus><Children>2</Children></Customer>

Early Failing Requests

IDG

The early failing requests page displays a list of all requests that failed before invocation of a processing rule in the service.

The following information is available for each transaction:

Column	Description
FSH/Proxy	Front side handler of the service
Operation/URI	Operation type of this transaction (may show the Request URI for Multi-Protocol Gateway services)
Time	Time this transaction was logged
Device	The device this transaction ran on.
Domain	The domain this transaction ran in
Trans. ID	The monitored device's transaction id. Clicking the Transaction id link loads the Single Transaction details view
Client IP	The client originating the transaction. This can sometimes be the IP of the load balancer.

API CONNECT

The early failing requests page displays API Connect transactions that did not activate any APIs
The following information is available for each transaction (depends on the transactions, not all columns will contain data)

Column	Description
API Name	The API Name that was run, or "Unknown" if no API was started
Time	Time this transaction was logged
Device	The device this transaction ran on.
Domain	The domain this transaction ran in
Catalog Name	The API Connect Catalog Name the transaction ran in
Space Name	The API Connect Space Name the transaction ran in
App Name	The API Connect App Name the transaction ran in
Client ID	The API Connect Client ID
Trans. ID	The monitored device's transaction id. Clicking the Transaction id link loads the API Connect Single Transaction details view
Client IP	The client originating the transaction. This can sometimes be the IP of the load balancer.
Gl. Trans ID	The global transaction Id of the transaction

Extended Transactions

Extended Transactions, which are transactions that span more than one monitored service/domain/device, are being tracked in a non-intrusive way over HTTP protocol. This correlation is defined by means of a global transaction ID.

Examples of extended transactions include:

- A DMZ gateway relays a request into the LAN internal gateway. The request transcends two machines and would have consists of two separate transactions.
  With the Extended Transaction, you can treat this operation as a single one.
- An extended transaction may span domains inside a single gateway or across several gateways.

The following information is available for each extended transaction:

Column	Description
Service Name	The service the first transaction ran on
Operation/URI	The operation’s name for this first transaction or URI
Time	Timestamp for the first transaction.
Device Name	The device this first transaction ran on
Domain	The domain this first transaction ran on
Status	The status for the first transaction. The possible values are • OK • ERROR
Error Message	When the extended transaction completed in an error state, this column will hold the error message
Client IP	The client IP of the machine (or load balancer) where this transaction started.
Steps	Indicates the number of transactions that are part of the extended transaction
Gl. Trans. ID	Correlation ID between transactions across services/domains/devices
Elapsed (ms)	The number of milliseconds the extended transaction spanned.

Click the ⊞ icon to the left of an extended transaction to open a panel with extra information relating the single transactions comprising it:

Column	Description
Service Name	The service this transaction ran on.
Time	Timestamp for the transaction.
Device Name	The device this transaction ran on
Domain	The domain the transaction ran on
Status	The status for this transaction. The possible values are: • OK • ERROR
Error Message	If the transaction ended in an error state, this column will hold the error message received. If the error message is too long, it will be abbreviated, with an ellipsis at the end. Hovering over a abbreviated message will display the full message in a pop-up
Transaction Id	The Transaction id. Click on the transaction id to open a single transaction view for this transaction
Elapsed (ms)	Total elapsed time, the number of milliseconds the transaction took.

Network Elapsed (ms)	Network elapsed time
Device Elapsed (ms)	DataPower processing elapsed time
Back-End Elapsed (ms)	Back-End processing elapsed time

LIMITATIONS

Currently (v1.0.8.0) this feature is enabled by default only for new installations.

Deprecated Extended Transactions

The intrusive Extended Transaction functionality will be deprecated in the near future

Extended Transactions are defined by the administrator over a web service proxy.

DPOD allows correlation between transactions across domains. This correlation is defined by means of a correlation id.
Examples of extended transactions include:

- A DMZ DataPower relays a request into the LAN internal DataPower. The request transcends two machines and would have consists of two separate transactions. With a DPOD Extended Transaction, you can treat this operation as a single one.
- An extended transaction may span domains inside a single DataPower machine or across several machines.

The following information is available for each extended transaction:

Column	Description
Service Name	The service this extended transaction ran on
Operation	The operation's name for this extended transaction
Time	Timestamp for the extended transaction. This will be the timestamp for the last response within the extended transaction
Status	The status for the extended transaction. The possible values are • OK • INPROCESS • ERROR
Error Message	When the extended transaction completed in an error state, this column will hold the error message.
Client IP	The client IP of the machine (or load balancer) where this transaction started.
Elapsed (ms)	The number of milliseconds the extended transaction spanned.

Click the ➕ icon to the left of an extended transaction to open a panel with the extended transaction's correlation Id at the top, and extra information relating the single transactions comprising it:

Column	Description
Service Name	The service this transaction ran on. This may be the same service name listed for the extended transaction, or a different service name.
Rule	The type of the transaction within the extended transaction. The possible values are: • Request • Response • Error
Device Name	The device this transaction ran on
Status	The status for this transaction. The possible values are: • OK • INPROCESS • ERROR
Domain	The domain the transaction ran on
Time	Timestamp for the transaction.
Transaction Id	The Transaction id. Click on the transaction id to open a single transaction view for this transaction

Error Message	If the transaction ended in an error state, this column will hold the error message received. If the error message is too long, it will be abbreviated, with an ellipsis at the end. Hovering over a abbreviated message will display the full message in a pop-up.
Elapsed (ms)	The number of milliseconds the transaction took.

Payload Capture

The Payload Capture page shows Active WS-M subscriptions, allows the user to stop active subscriptions and create new subscriptions.

> This Payload Capture page only shows and manages subscription that were created by DPOD

VIEW OR STOP ACTIVE WS-M SUBSCRIPTIONS

The Payload Capture page shows a list of currently active WS-M subscription

Column	Description
Device	The device where the WS-M subscription was started
Domain	The domain where the WS-M subscription was started
User Name	The user name who created the subscription
Start Time	When the subscription was started
End Time	When the subscription will end (the subscription will end automatically)
Subscription Id (Context Id)	The DataPower Id of the subscription
Stop Subscription	Stop the subscription. Every user that has access to the page (and has permission to view the device/domain) may stop a subscription, even if it was created by another user or by an admin

CREATE SUBSCRIPTION

Click the "Create Subscription" button (on the top-right) to create a new subscription

Enter the Device and Domain names, and Duration in Minutes (up to the maximum duration defined by the system administrator)

You may choose multiple devices or domains, or use an asterisk as a wildcard in the domain or device names.
For example, choosing QA* for the device name and DMZ for the domain name, will record payloads for all DMZ domains in devices QA1, QA2 and QA3.

> As payload capture may cause high load on the monitored device - you can not use an asterisk to choose all devices or all domain

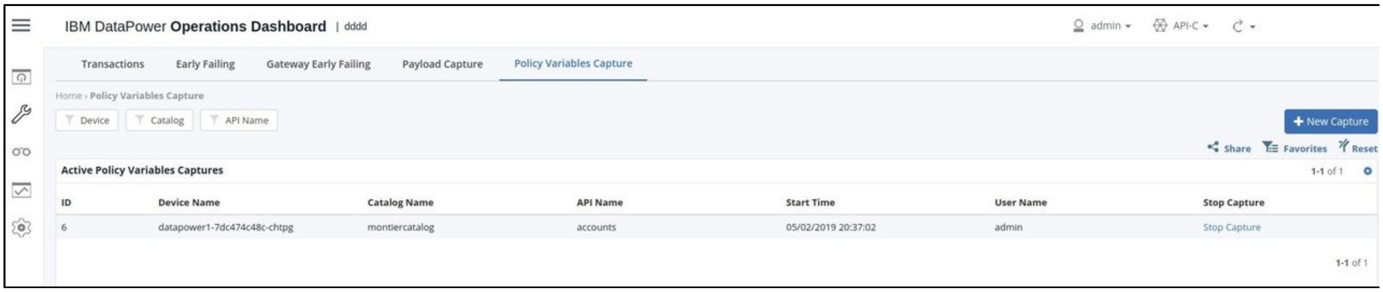
PERMISSIONS AND SETTINGS

Please refer to the Payload Capture Settings and Authorization page in the admin guide.

Policy Variables Capture (API-C only)

Policy Variables Capture will capture the values of the API assembly's "set-variable" policy variables and optionally capture DataPower's context name variables.

> Policy Variables Capture may have a performance impact.
> The variables names and values are not encrypted, this feature should only be used for troubleshooting and not for auditing.



Active Policy Variables Captures

1-1 of 1

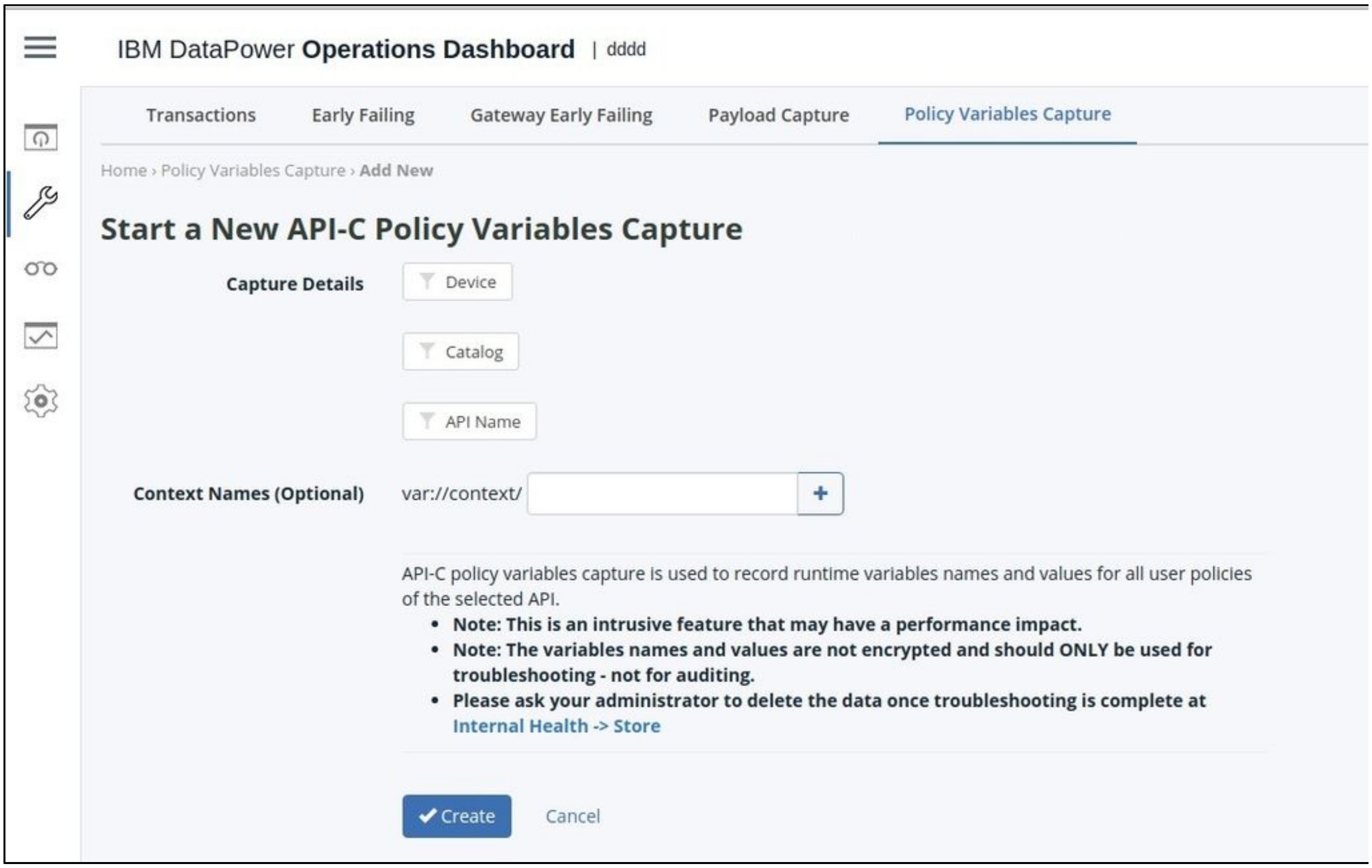
ID	Device Name	Catalog Name	API Name	Start Time	User Name	Stop Capture
6	datapower1-7dc474c48c-chtpg	montiercatalog	accounts	05/02/2019 20:37:02	admin	Stop Capture

1-1 of 1

The Policy variables capture page shows the currently active captures and allows to start new captures.
The capture will run on all transaction of a specific API Name from a specific Catalog that runs on the device.
The capture will run indefinitely until manually stopped from this page (use the "Stop Capture" button).

> Only 2 policy captures are allowed simultaneously per device

Click "New Capture" to start a new capture, enter the capture details (no wildcards are allowed)
You may also add a DataPower's context name to capture (var://context/myContext)



Start a New API-C Policy Variables Capture

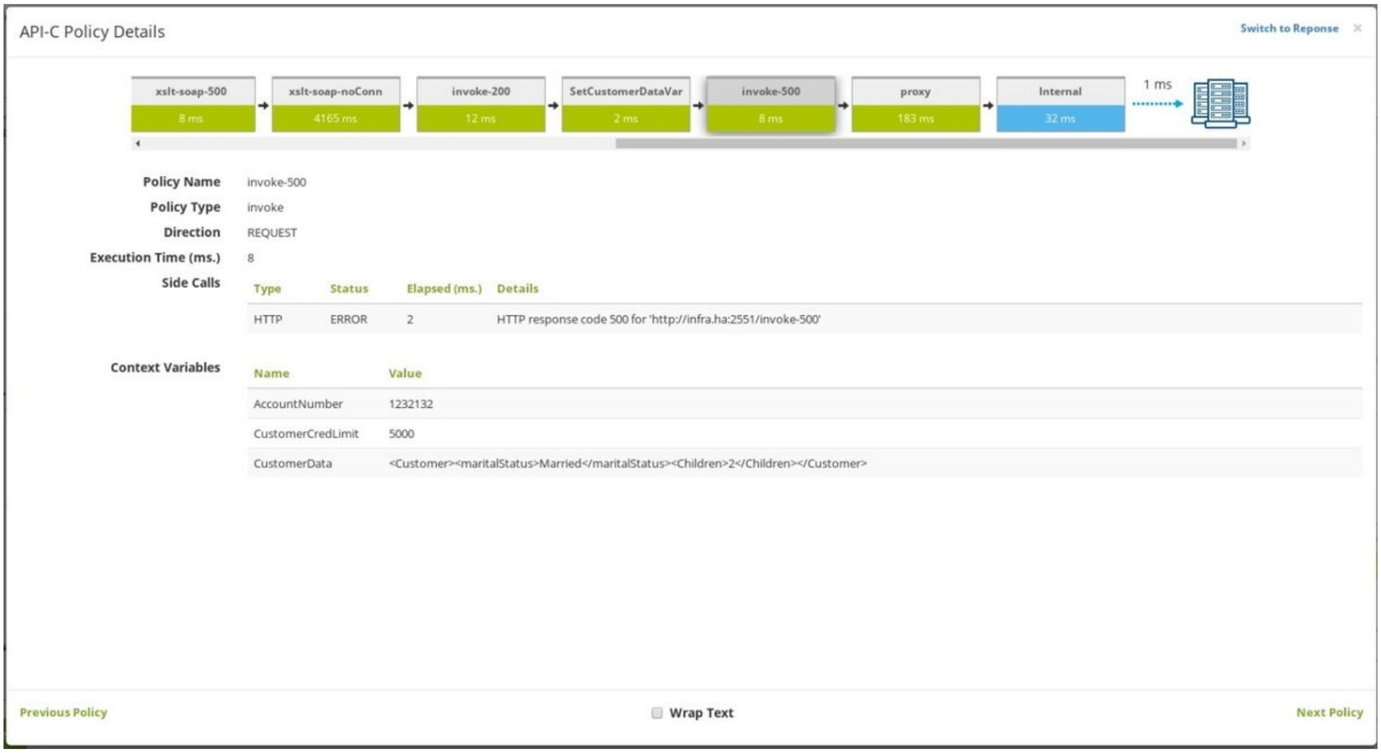
Capture Details

Context Names (Optional) var://context/

API-C policy variables capture is used to record runtime variables names and values for all user policies of the selected API.

- **Note: This is an intrusive feature that may have a performance impact.**
- **Note: The variables names and values are not encrypted and should ONLY be used for troubleshooting - not for auditing.**
- **Please ask your administrator to delete the data once troubleshooting is complete at Internal Health -> Store**

The values will be displayed in the Policy Details Window in the API Connect Single Transaction page under "Context Variables".
The capture is limited in size to 2kb of variable names data and 2kb of variable values data, an informational message will appear above the context variables list if some variable names or values were not included.



Policy Name	invoke-500
Policy Type	invoke
Direction	REQUEST
Execution Time (ms.)	8

Side Calls

Type	Status	Elapsed (ms.)	Details
HTTP	ERROR	2	HTTP response code 500 for 'http://infra.ha:2551/invoke-500'

Context Variables

Name	Value
AccountNumber	1232132
CustomerCredLimit	5000
CustomerData	<Customer><maritalStatus>Married</maritalStatus><Children>2</Children></Customer>

PERMISSIONS AND RETENTION

Please refer to the Policy Variables Capture Settings and Authorization page in the admin guide.

Explore

The Explore view contains the following tabs:

Service Configuration and Change Audit

Failed Objects (DataPower objects that are enabled in configuration but in "Down" state)

Service Configuration

The Service Configuration tab in the Explore view lists all the services that were discovered by DPOD in your monitored devices.

DPOD currently discovers services of the following types:

- Web Service Proxy
- Multi-Protocol Gateway
- XML Firewall
- SSL Proxy
- TCP Proxy
- B2B Gateway (and the corresponding B2B Partner Profiles)

DPOD scans your monitored devices for new services every 30 minutes (you can change this interval from the system parameters page)

The service details are shown in a table:

> Each service's front-side handler is shown separately in the table.
>
> For example, a Multi-Protocol Gateway service with HTTP front side handler an an IBM MQ front side handler - will be shown twice in the table, once per FSH.

Column	Description
Device	The device the service is configured on. Click on the device name to apply a device-filter to the table.
Domain	The domain the service is configured on. Click on the domain name to apply a domain-filter to the table.
Service Name	The name of the service. Click on the service name to apply a service-filter to the table. As services may be configured on more than one domain, this does not automatically load the single-service view.
Front-Side Handler	The Front-Side handler that handles this service. Click the front-side handler name to apply a front-side handler filter to the table.
Service Type	The type of the service (and SOAP version where applicable). Click on the service type to apply a service-type filter to the table.
Front URI	The front-end URI (where applicable)

SINGLE SERVICE VIEW

Click a table row to drill down into a single-service view - the Service Details page (or B2B Gateway Details for B2B objects) . From there, you can view the service configuration and change audit information

IMPACT ANALYSIS

You may also use the Explore view to search the configuration and perform impact analysis on your system.
Example

Use Explore to analyze which services will be impacted if you make a change to a Front Side Handler's port.

Service Details

The service details view is displayed when you have filtered the table on the Explore view down to a single service. This view is composed of two widgets:

Service Configuration

This widget contains full configuration details of the service as DPOD views it:

Heading	Description
Device	The device this service is deployed on
Domain	The domain this service is deployed on
Service	The service name
FS Handler	The Front-Side Handler for this service
Service Type	The type of service. (for example, MultiProtocolGateway, XMLFirewallService, etc)
SOAP Version	SOAP Version for this service (where applicable)
Admin State (Svc)	The Administrative state of this service (enabled / disabled)
Admin State (FSH)	The Administrative state of the front-side handler (where applicable).
F. Protocol / B. Protocol	Front / Back end protocol this service runs on.
F. Address / B. Address	Front / Back end IP Address for this service.
F. Port / B. Port	Front / Back end TCP port for this service
F. URI / B. URI	Front / Back end URI for this service
F. QMGR / B.QMGR	Front / Back end Queue Manager for this service (when relevant)
F. QMGR Group / B. QMGR Group	Front / Back end Queue Manager Group for this service (when relevant)
F. Request Q. / B. Request Q.	Front / Back end Request Queue
F. Reply Q. / B. Reply Q.	Front / Back end Reply Queue
Comments	The "User comments" field (sometimes called "Summary field") of the service

Change Audit

The Change Audit widget lists all changes made to the service. These may be changes to services, front-side handlers, B2B Gateways and B2B Partners.
DPOD queries the DataPower every 30 minutes for all services' configuration (the interval may be changed from the system parameters page), compares the result with the previous configuration and stores a change audit record when changes are found.

The Change Audit is displayed in a table, where each row describes a single change:

Column	Description
Time Sampled	The change’s timestamp sampled by DPOD

Change Operation	The change operation (for B2B Gateway objects the change operation will also contain the B2B partner's name if applicable). For example - "Replaced in FSH" for an attribute that was changed in a the front-side handler "Removed in Service" for an attribute that no longer exists in a Service The "Discovered" operation describes when the service/FSH was first discovered by DPOD, and not the time it was originally created
Description	Description of the change For example - **User Comments** was changed from old text to new text **Admin State** was changed from enabled to disabled
Latency Change	The change in latency (percentage) before and after the configuration change with a time interval of 4 hours, or n/a if there were no executions of the tx.
Error Change	The change in errors (percentage) before and after the configuration change with a time interval of 4 hours, or n/a if there were no errors before or after the change.

B2B Gateway Details

This page contains configuration details of the B2B Gateway as DPOD views it,
It is composed from three sections:

B2B Gateway Configuration

Heading	Description
Device	The device this B2B Gateway is deployed on
Domain	The domain this B2B Gateway is deployed on
Service	The B2B Gateway name
FS Handler	The Front-Side Handler
Service Type	Always "B2BGateway"
Admin State (GW)	The Administrative state of the B2B Gateway (enabled / disabled)
Admin State (FSH)	The Administrative state of the front-side handler
F. Protocol / B. Protocol	Front / Back end protocol this service runs on.
F. Address / B. Address	Front / Back end IP Address
F. Port / B. Port	Front / Back end TCP port
F. URI / B. URI	Front / Back end URI
F. QMGR / B.QMGR	Front / Back end Queue Manager (when applicable)
F. QMGR Group / B. QMGR Group	Front / Back end Queue Manager Group (when applicable)
F. Request Q. / B. Request Q.	Front / Back end Request Queue (when applicable)
F. Reply Q. / B. Reply Q.	Front / Back end Reply Queue (when applicable)
Comments	The "Comments" field

B2B Partners

Heading	Description
Partner Name	The B2B Partner Profile's name
Admin State	The Administrative state of the B2B Partner Profile (enabled / disabled)
Enabled	On of Off
Partner Group	The name of the B2B Profile group (where a partner is part of a group)
Type	External or Internal
Processing Policy	The Processing Policy's name
Comments	The "Comments" field
Business Ids	A list of the all Partner Business Ids
DUNS Business Ids	A list of the all Partner Business Ids (DUNS)
DUNS+4 Busniess Ids	A list of the all Partner Business Ids (DUNS+4)
Partner Email Addresses	A list of all the Partner Email addresses

Destinations	a list containing all the Partner Destinations, Showing: The destination's name The destination URL Email address (where applicable)

Change Audit

Please refer to the change audit section of the Service Details page

Service Configuration Changes

The Service Configuration Changes tab in the Explore view lists all changes made to the services ordered by time descending.

These may be changes to the gateway's services, front-side handlers, B2B Gateways and B2B Partners.
DPOD queries the gateway every 30 minutes for all services' configuration (the interval may be changed from the system parameters page), compares the result with the previous configuration and stores a change audit record when changes are found.

The Change Audit is displayed in a table, where each row describes a single change:

Column	Description
Device	The device the service is configured on. Click on the device name to apply a device-filter to the table.
Domain	The domain the service is configured on. Click on the domain name to apply a domain-filter to the table.
Service Name	The name of the service. Click on the service name to apply a service-filter to the table.
Time Sampled	The change’s timestamp sampled by DPOD
Change Operation	The change operation (for B2B Gateway objects the change operation will also contain the B2B partner's name if applicable). For example - "Replaced in FSH" for an attribute that was changed in a the front-side handler "Removed in Service" for an attribute that no longer exists in a Service The "Discovered" operation describes when the service/FSH was first discovered by DPOD, and not the time it was originally created
Description	Description of the change For example - **User Comments** was changed from old text to new text **Admin State** was changed from enabled to disabled
Latency Change	The change in latency (percentage) before and after the configuration change. The time interval before and after can be set by the Latency/Error filter (4 hours, 1 day, 1 week). n/a will be displayed if there were no executions of the service.
Error Change	The change in errors (percentage) before and after the configuration change. The time interval before and after can be set by the Latency/Error filter (4 hours, 1 day, 1 week). n/a will be displayed if there were no errors before or after the change.

Failed Objects

The Failed Objects page shows details about DataPower object that are enabled in configuration but in operational state "Down".

By default, DPOD checks for failed objects every 5 minutes, you can change this interval from the System Parameters page ("Interval in Seconds to Monitor Objects Status" option)

Column	Description
Time Detected	When the object was last sampled
Device	The Device name
Domain	The Domain name
Object Name	The DataPower object name
Object Class	The Object's class
Operational State	Always "down"
Admin State	Always "enabled"
Event Code	The Event code returned from the DataPower
Error Code	The Error code returned from the DataPower

SCANNED OBJECT CLASSES

By default, DPOD only scans the status for following object classes:

> You can make DPOD scan all objects by changing the "Object Status Monitor Should Only Check Common Object Classes" option to "false" from the System Parameters page

AS2SourceProtocolHandler
AS3SourceProtocolHandler
B2BGateway
CertMonitor
ClusterService
CryptoFWCred
CryptoIdentCred
CryptoKerberosKDC
CryptoKerberosKeytab
CryptoKey
CryptoProfile
CryptoValCred
DNSNameService
DomainAvailability
EthernetInterface
FTPFilePollerSourceProtocolHandler
FTPServerSourceProtocolHandler
HTTPService
HTTPSourceProtocolHandler
HTTPSSourceProtocolHandler
IMSConnect
IMSConnectSourceProtocolHandler
LDAPConnectionPool
LLMSourceProtocolHandler
LogTarget
MgmtInterface
MQFTESourceProtocolHandler
MQGW
MQhost
MQproxy
MQQM
MQQMGroup
MQSourceProtocolHandler
MultiProtocolGateway
NetworkSettings

NFSDynamicMounts
NFSFilePollerSourceProtocolHandler
NFSStaticMount
NTPService
OAuthSupportedClient
OAuthSupportedClientGroup
PeerGroup
POPPollerSourceProtocolHandler
RaidVolume
RBMSettings
SecureCloudConnector
SNMPSettings
SQLDataSource
SSHClientProfile
SSHServerSourceProtocolHandler
SSLProxyProfile
SSLProxyService
StatelessTCPSourceProtocolHandler
Statistics
SystemSettings
TAM
TelnetService
Throttler
TibcoEMSSourceProtocolHandler
TimeSettings
TraceTarget
UDDIRegistry
VLANInterface
WebB2BViewer
WebGUI
WebSphereJMSServer
WebTokenService
WSGateway
XMLFirewallService
XMLManager
XSLCoprocService
XSLProxyService
XTCProtocolHandler
AS1PollerSourceProtocolHandler
CryptoCertificate
CryptoSSKey
EBMS2SourceProtocolHandler
ErrorReportSettings
IMSCalloutSourceProtocolHandler
LoadBalancerGroup
NFSClientSettings
RADIUSSettings
SFTPFilePollerSourceProtocolHandler
SSHService
TCPProxyService
TRVSourceProtocolHandler
WebAppFW
WebSphereJMSSourceProtocolHandler
WSRRServer

DevOps Services Portal

> System administrators should also consult the DevOps Portal Setup and Security section

The DevOps services portal enables users to view all the services in the monitored devices and perform predefined actions on the services.

DPOD allows the following actions:

1. Validate Remote WSDL
2. Promote Remote WSDL
3. Validate Local WSDL
4. Promote Local WSDL
5. Stop Service
6. Start Service
7. Import Service

DevOps Services List

The services list displays a list of all services in the monitored devices.
The data in this list is sourced from the service configuration sampling which runs every 30 minutes by default, and is therefore not real-time.
An admin can change the sampling interval from the system parameters page. The interval should be at least 10 minutes.

Column	Description
Service Name	The service name
Device Name	The monitored device name
Domain Name	The domain name
Service Type	The service type. The service configuration currently samples the following service types: • Web Service Proxy • Multi-Protocol Gateway • XML Firewall • SSL Proxy • TCP Proxy • B2B Gateway (and the corresponding B2B Partner Profiles)
User Description	A service description that may be set by a system administrator, see DevOps Portal Setup and Customization for more details
Operation Status	See "Operation Status" below

Click the expand icon ⊞ to show additional details about the service (For Web Service Proxy Services):

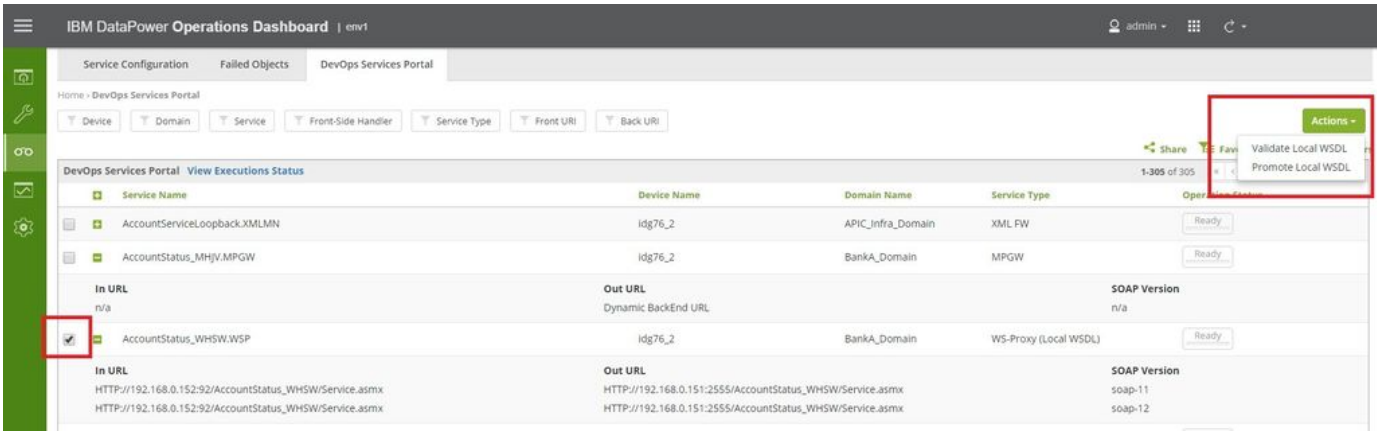
Column	Description
In URL	The URL that is bound to the service
Out URL	The URL of the backend or "Dynamic URL"
SOAP Version	The service's SOAP version

Click the expand icon ⊞ on the table's header to expand all services.

Starting a DevOps Action

Choose a service by selecting the checkbox on its left and click the "Actions" button to show available actions for this service.
Only one action may be performed on a service at one time.

> Selecting multiple services at once is supported only for the stop or start service actions.
> You may not see any available actions in the drop-down, depends on your permissions and system settings.



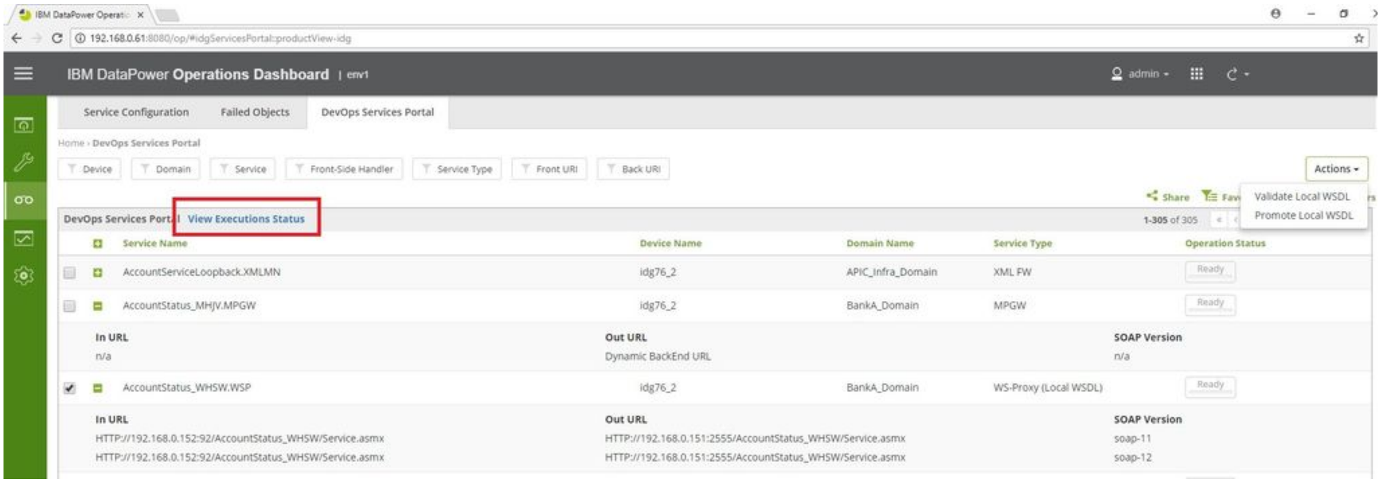
	⊞	Service Name	Device Name	Domain Name	Service Type	Operation Status
□	⊞	AccountServiceLoopback.XMLMN	idg76_2	APIC_Infra_Domain	XML FW	Ready
□	⊟	AccountStatus_MHJV.MPGW	idg76_2	BankA_Domain	MPGW	Ready

In URL	Out URL	SOAP Version
n/a	Dynamic BackEnd URL	n/a

☑	⊟	AccountStatus_WHSW.WSP	idg76_2	BankA_Domain	WS-Proxy (Local WSDL)	Ready

In URL	Out URL	SOAP Version
HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-11
HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-12

Click on "View execution status" link in the list's header to go to the execution status page for all services



IBM DataPower Operations Dashboard | env1

Service Configuration | Failed Objects | DevOps Services Portal

Home › DevOps Services Portal

DevOps Services Portal | View Executions Status

1-305 of 305

		Service Name	Device Name	Domain Name	Service Type	Operation Status
□	⊞	AccountServiceLoopback.XMLMN	idg76_2	APIC_Infra_Domain	XML FW	Ready
□	⊟	AccountStatus_MHJV.MPGW	idg76_2	BankA_Domain	MPGW	Ready
☑	⊟	AccountStatus_WHSW.WSP	idg76_2	BankA_Domain	WS-Proxy (Local WSDL)	Ready

AccountStatus_MHJV.MPGW:

In URL	Out URL	SOAP Version
n/a	Dynamic BackEnd URL	n/a

AccountStatus_WHSW.WSP:

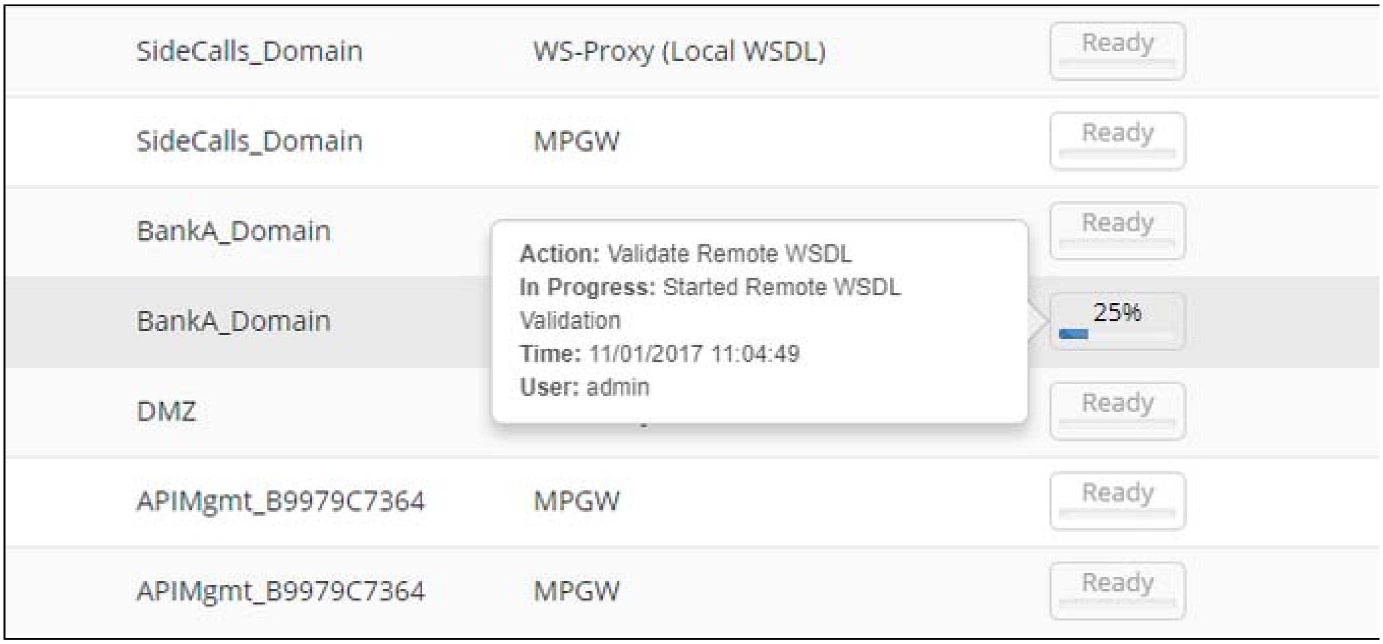
In URL	Out URL	SOAP Version
HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-11 soap-12

The Operation Status Column

When an action is running, its progress is displayed in the operation status column of the service.
When no operation is currently executing, the column displays the results of the latest operation (within the last 30 minutes)
When no operation is currently running, and no operations were executed in the last 30 minutes, a "ready" prompt is displayed.

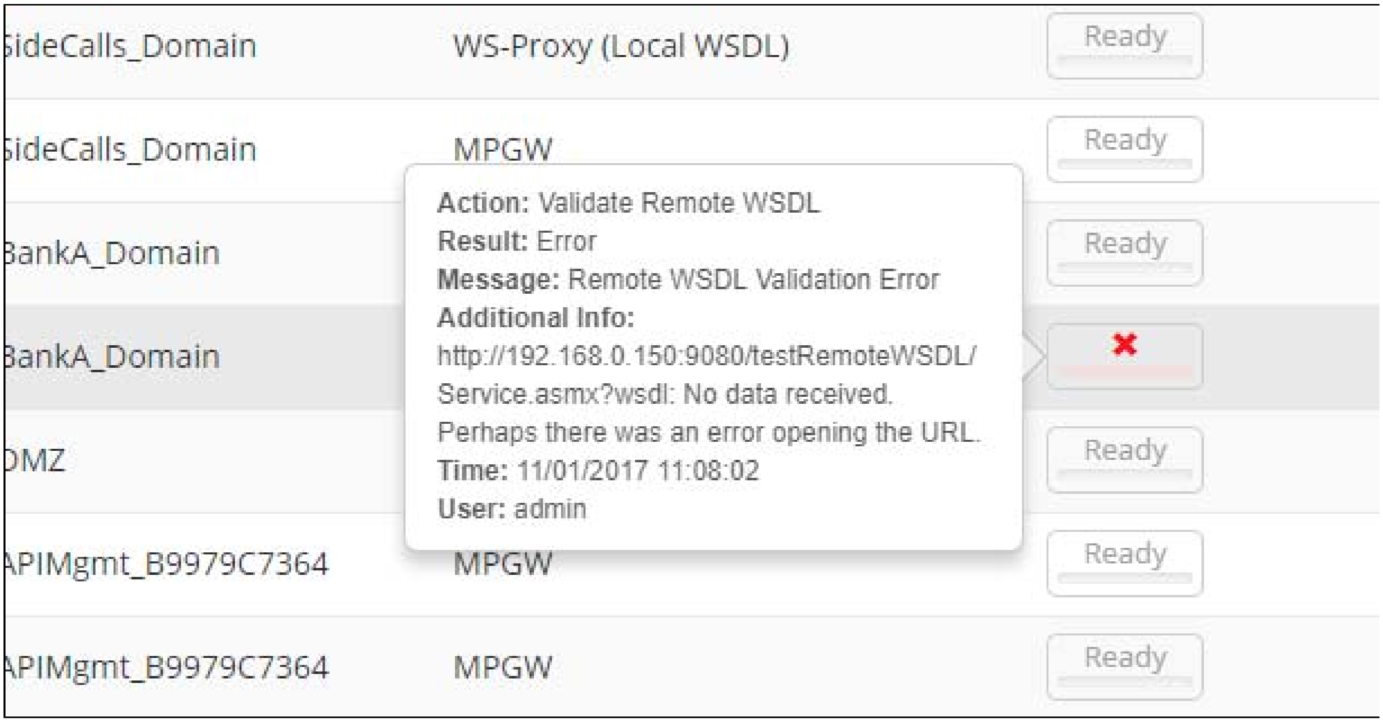
Click on the operation status to navigate to the execution status page where the current and previous executions are listed.

Hover over the icon to show additional details and/or error messages



SideCalls_Domain	WS-Proxy (Local WSDL)	Ready
SideCalls_Domain	MPGW	Ready
BankA_Domain		Ready
BankA_Domain		25%
DMZ		Ready
APIMgmt_B9979C7364	MPGW	Ready
APIMgmt_B9979C7364	MPGW	Ready

Action: Validate Remote WSDL
In Progress: Started Remote WSDL Validation
Time: 11/01/2017 11:04:49
User: admin



SideCalls_Domain WS-Proxy (Local WSDL) Ready

SideCalls_Domain MPGW Ready

BankA_Domain Ready

BankA_Domain ✖

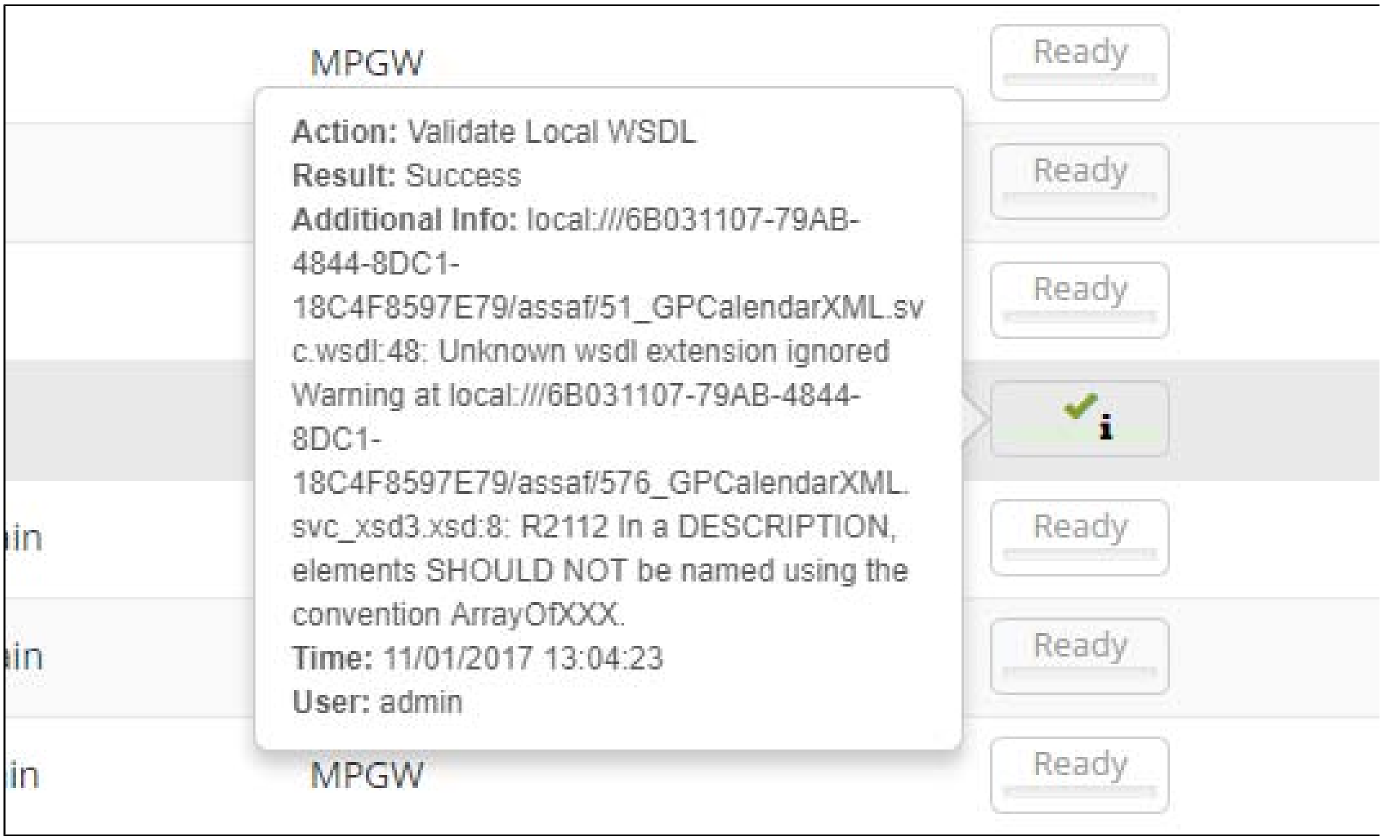
DMZ Ready

APIMgmt_B9979C7364 MPGW Ready

APIMgmt_B9979C7364 MPGW Ready

Action: Validate Remote WSDL
Result: Error
Message: Remote WSDL Validation Error
Additional Info:
http://192.168.0.150:9080/testRemoteWSDL/Service.asmx?wsdl: No data received. Perhaps there was an error opening the URL.
Time: 11/01/2017 11:08:02
User: admin

If an operation was successful, but additional data was generated (such as WSDL compilation warnings) - a small ℹ Icon will appear next to the result icon.
Hover over the icon to show the complete message, or click the icon to go to the execution status page



MPGW Ready

Ready

Ready

✓ℹ

in Ready

in Ready

in MPGW Ready

Action: Validate Local WSDL
Result: Success
Additional Info: local:///6B031107-79AB-4844-8DC1-18C4F8597E79/assaf/51_GPCalendarXML.svc.wsdl:48: Unknown wsdl extension ignored Warning at local:///6B031107-79AB-4844-8DC1-18C4F8597E79/assaf/576_GPCalendarXML.svc_xsd3.xsd:8: R2112 In a DESCRIPTION, elements SHOULD NOT be named using the convention ArrayOfXXX.
Time: 11/01/2017 13:04:23
User: admin

DevOps Action Executions Status Page

The DevOps Actions Executions Status page shows the following details for each execution:

Column	Description
ID	The internal ID of the execution, it may be used when searching DPOD logs to investigate a problem
Request Time	The time when the action was first requested by the user
Device	The service's device
Domain	The service's domain
Service	The service's name
Action	The requested action
Result	The action result (Requested, In Progress, Success, Error, Warning)
Message	The latest info/error message returned for the action
Additional Info	Any additional message, such as WSDL validation warnings
Last Status Time	The last time when the action was updated
Requesting User	The DPOD user that requested the action
Execution UUID	Internal identifier for this execution. This will also be the name of the temporary service that was created by DPOD for remote/local WSDL validations in the temporary domain.

Additional information may be available when hovering over a table's row.

For remote WSDL validation/promotion:
Change WSDL Location: true / false
New WSDL Location: (only if "Change WSDL Location" is true) the requested address of the new WSDL

Additional information for import service:
OpState Before / OpState After: up / down
AdminState Before / AdminState After: enabled / disabled
Import File Name: The import file's name that was uploaded by the user
Deployment Policy: The deployment policy that was selected by the user before the execution, it may have been overridden during execution by the admin's custom script
Dry Run Requested: true / false

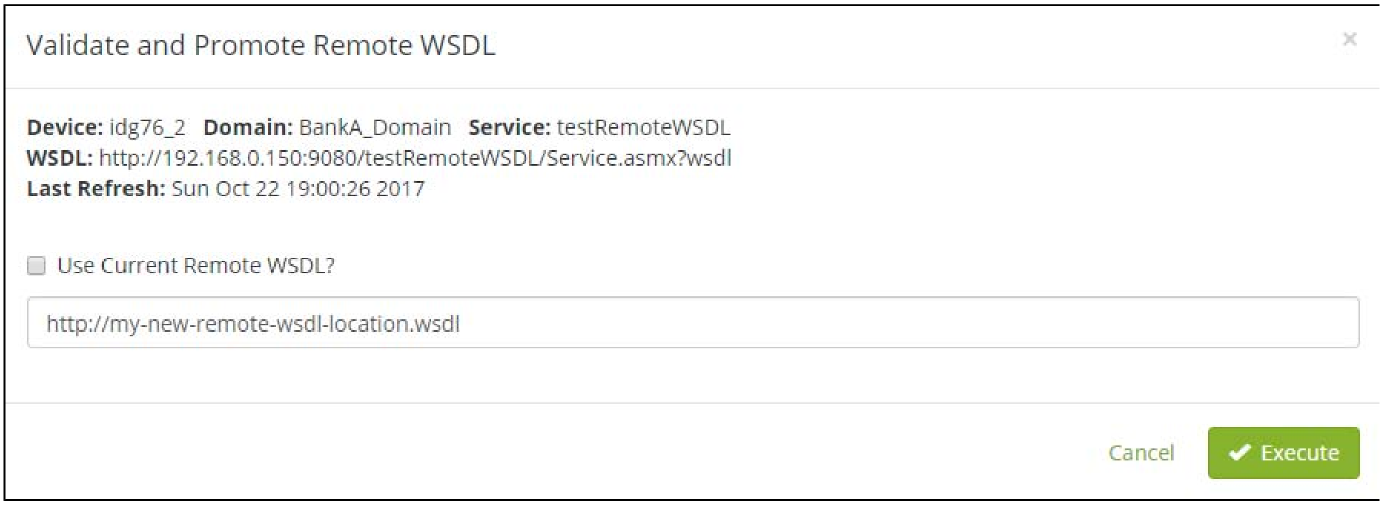
Remote WSDL Validation and Promotion

The remote WSDL promotion refreshes the service's WSDL, or replaces a current remote WSDL address with a new address.

Initiating a New Validate or Promote Remote WSDL Request

Choose either Validate Remote WSDL or Promote Remote WSDL from the DevOps Services List to initiate the process

1. Changing a service with Local WSDL to a remote WSDL or vice versa is not supported
2. You may or may not be able to enter a new remote WSDL address, depending on your permissions
3. Validate/Promote of remote WSDL over HTTPS is not supported



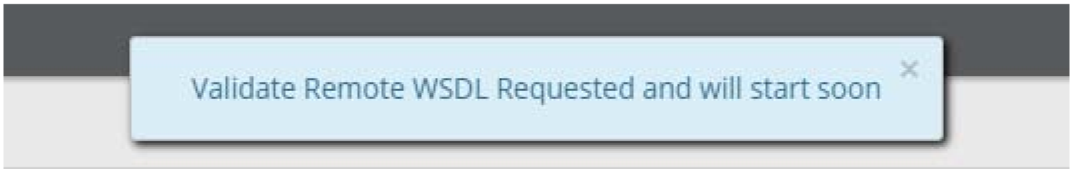
Validate and Promote Remote WSDL

Device: idg76_2 **Domain:** BankA_Domain **Service:** testRemoteWSDL
WSDL: http://192.168.0.150:9080/testRemoteWSDL/Service.asmx?wsdl
Last Refresh: Sun Oct 22 19:00:26 2017

□ Use Current Remote WSDL?

http://my-new-remote-wsdl-location.wsdl

Click on Execute to send the request



Validate Remote WSDL Requested and will start soon

DPOD's internal process will monitor and start executing pending requests every one minute.

Validation Flow

1. DPOD will use a temporary domain on a monitored device that was chosen and created by the admin.
2. DPOD creates a temporary service on the temporary domain that points to the remote WSDL (or to the new remote WSDL address if the user requested to change the WSDL address).
3. The new temporary service will be created without any front side handlers.
4. After creating the temporary service, DPOD will check the temporary service's WSDL compilation status.

Promotion Flow - Remote WSDL Promotion (Same Address)

1. DPOD first runs the validation flow and will continue to step 2 only if the validation was successful
2. Perform a DataPower WSDL Refresh

Promotion Flow - Remote WSDL Promotion (Address Change)

1. DPOD first runs the validation flow and will continue to step 2 only if the validation was successful
2. DPOD exports the original service
3. DPOD changes the WSDL address in the export to the new remote WSDL address
4. DPOD Imports the origin service again with the new WSDL address.
5. DPOD checks the WSDL status and the service operational state
6. If the service is not up or the WSDL status is not ok - DPOD tries to rollback the operation by importing the service again with the original unchanged WSDL address

Local WSDL Validation and Promotion

The local WSDL promotion replaces the current service WSDL and XSD with new files supplied by the user.

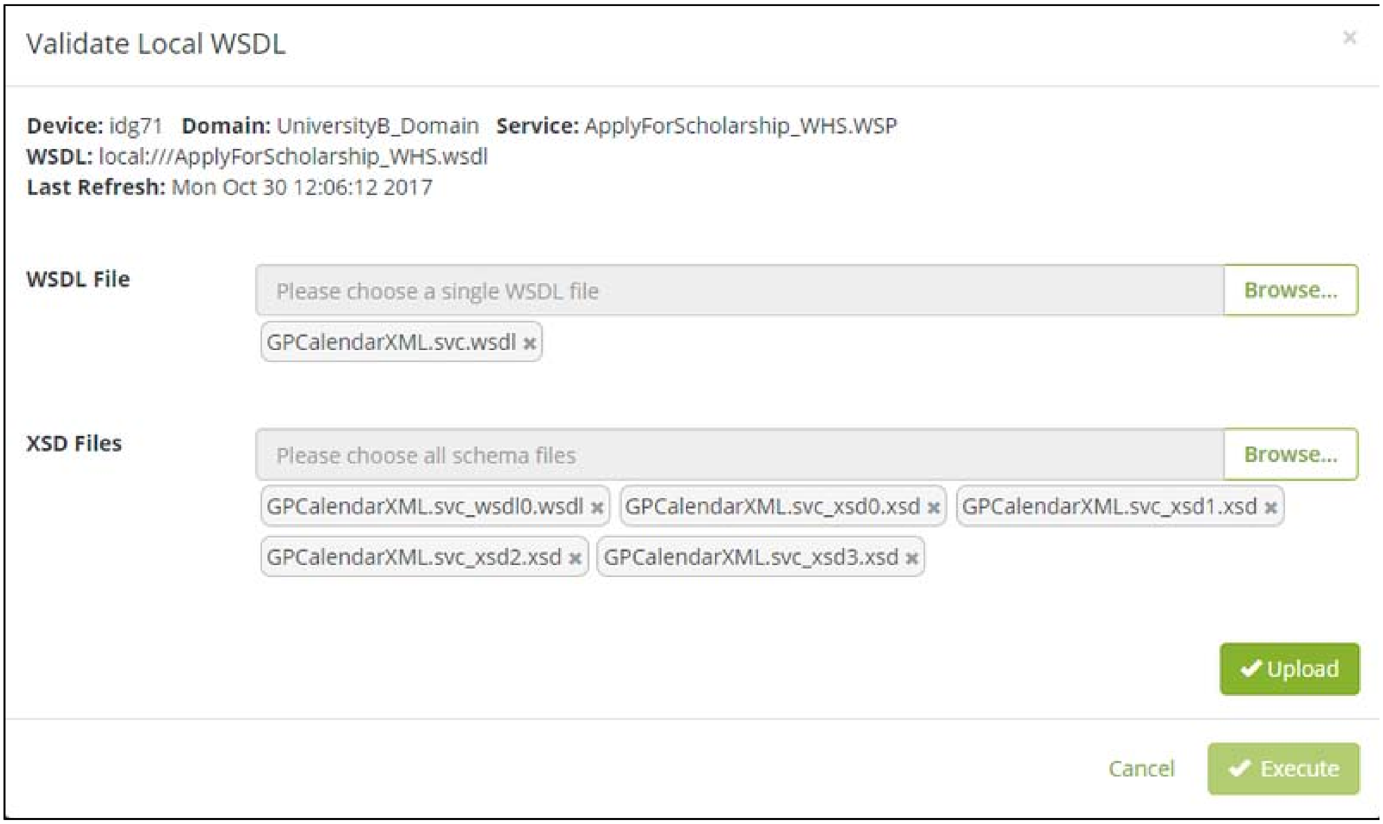
> In some cases, depending on the WSDL contents, the old WSEndpointRewritePolicy that is attached to the WS-Proxy can not be used with the new WSDL.
> In those cases, the Front-Side Handlers may need to be **re-added manually** to the WS-Proxy after the WSDL promotion is done.

Initiating a New Validate or Promote Local WSDL Request

Choose either Validate Local WSDL or Promote Local WSDL from the DevOps Services List to initiate the process

> Changing a service with Local WSDL to a remote WSDL or vice versa is not supported

> DPOD only supports WSDL/XSD files that are located in the local:/// directory
> DPOD does not support files in other locations such as the store:/// or temp:/// directories



Validate Local WSDL

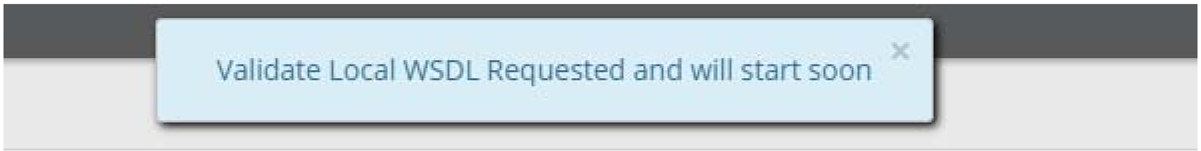
Device: idg71 **Domain:** UniversityB_Domain **Service:** ApplyForScholarship_WHS.WSP
WSDL: local:///ApplyForScholarship_WHS.wsdl
Last Refresh: Mon Oct 30 12:06:12 2017

WSDL File Please choose a single WSDL file — GPCalendarXML.svc.wsdl

XSD Files Please choose all schema files — GPCalendarXML.svc_wsdl0.wsdl, GPCalendarXML.svc_xsd0.xsd, GPCalendarXML.svc_xsd1.xsd, GPCalendarXML.svc_xsd2.xsd, GPCalendarXML.svc_xsd3.xsd

1. Choose one WSDL file
2. Choose zero or more XSD files (note that you can select multiple files at once from the XSD file browser).
3. Click "Upload" - this will upload your new files to DPOD (not to the DataPower!)
4. If the upload was successful, click on "Execute" to request a new WSDL validation/promotion

After clicking "Execute" the following message appears



Validate Local WSDL Requested and will start soon

DPOD's internal process will monitor and start executing pending requests every one minute.

Validation Flow

1. DPOD will use a temporary domain on a monitored device that was chosen and created by the admin.
2. First DPOD will execute a custom user script that will analyze the current service's WSDL and will return all the schema files used by the service
3. DPOD will download all the WSDL/XSD files of the current service
4. DPOD will execute a second custom user script to analyze the new WSDL/XSD files and replace all the references in the files so they point to the correct DataPower paths
5. DPOD will upload the new altered WSDL/XSD files to the temporary domain and create a new service that uses this WSDL
6. The new temporary service will be created without any front side handlers.
7. After creating the temporary service, DPOD checks the DataPower's WSDL compilation status.

> Messages from the validation steps may return DataPower errors or messages about service with a random name such as DD0396FC-D428-40E8-B64C-913824FD16D4 - this is the name of the temporary service used by DPOD.
> The same applies to messages about the WSDL/XSD validation, they will be uploaded to the temporary domain local storage in local:///temp-service-name/ (e.g. local:///DD0396FC-D428-40E8-B64C-913824FD16D4/)

Promotion Flow

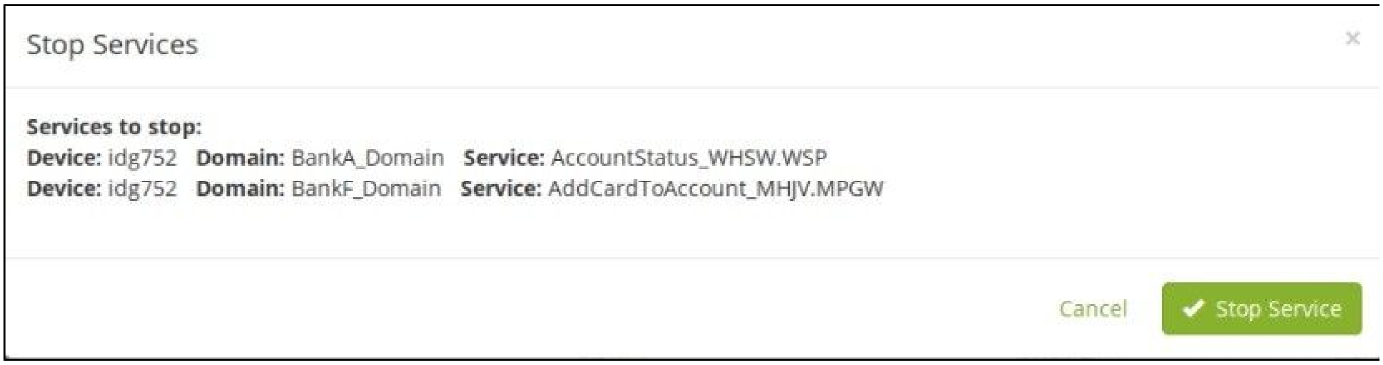
1. DPOD first runs the validation flow and will continue to step 2 only if the validation was successful
2. DPOD uploads the altered files from the validation steps to the DataPower, and creates any directories if needed.
   Existing files with identical names may be overriden.
3. DPOD exports the original service
4. DPOD changes the WSDL address in the export
5. DPOD imports the original service with the modified WSDL address.
6. DPOD checks the WSDL status and the service operational state
7. If the service is not up or the WSDL status is not ok - DPOD tries to rollback the operation by uploading the original WSDL/XSD files to local store and importing the service again with the original unchanged WSDL address

Stop or Start a Service

Stop or Start a DataPower service.

DPOD does not check the current status of the service, you may stop an already stopped service, or start an already started service.

The stop and start service actions can be performed on multiple services.



Stop Services

Services to stop:
Device: idg752 **Domain:** BankA_Domain **Service:** AccountStatus_WHSW.WSP
Device: idg752 **Domain:** BankF_Domain **Service:** AddCardToAccount_MHJV.MPGW

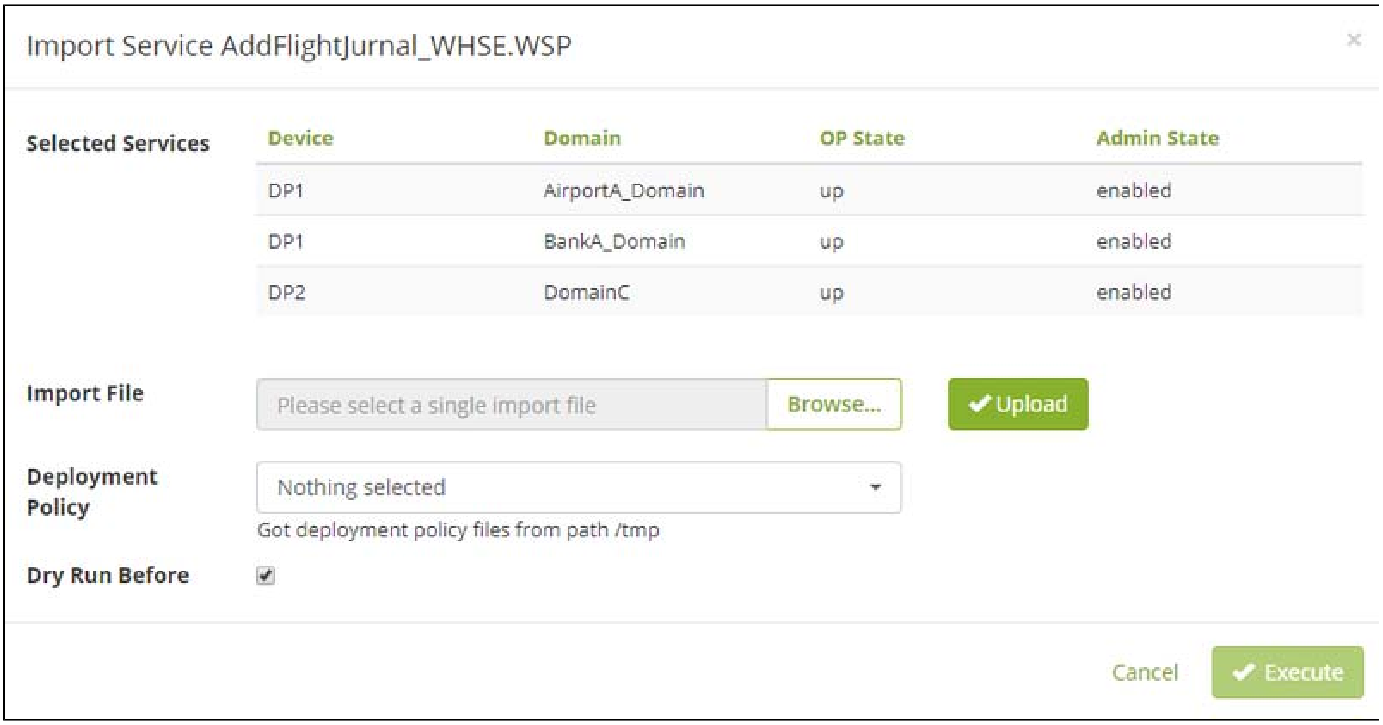
Import Service

The Import Service feature is designed to import one or multiple services from an export file.
You can import service(s) with the following limitations:

1. The export file (ZIP, XML or XCFG) should include only one service
2. You may only import export files of the same service and type (e.g. you can not import the export of WS-proxy-A or MPGW-B into WS-proxy-B)
3. The export file should not be a domain export
4. The import file size does not exceed the limit set by the system admin (the installation default is 10MB. system admins - please consult the DevOps Portal Setup and Customization section on how to change this value)

> All included objects will be overridden in the target service(s)

From the DevOps Services Portal services list, check one or more services and select "Import Service" from the Actions menu.



Import Service AddFlightJurnal_WHSE.WSP

Selected Services

Device	Domain	OP State	Admin State
DP1	AirportA_Domain	up	enabled
DP1	BankA_Domain	up	enabled
DP2	DomainC	up	enabled

Import File: Please select a single import file

Deployment Policy: Nothing selected

Got deployment policy files from path /tmp

Dry Run Before ☑

1. The top part of the window is informational and shows the current OP State and Admin State of the services, you may perform an import into service regardless of its OP or admin states.
2. Upload ZIP, XML or XCFG file containing the export.
3. The Deployment Policy selector may or may not be mandatory, according to the system admin setup (it is not mandatory by default. system admins - please consult the DevOps Portal Setup and Customization section on how to change this value)
   The Deployment Policy dropdown contains deployment policies that were pre-loaded into DPOD by the system admin, you cannot upload your own deployment policies.
4. Select "Dry Run Before" to execute the DataPower's dry-run import before the actual import, if any errors are returned from the dry-run - DPOD will stop and will not import the service.
5. Click on "Execute", the execute button will be grayed out if you did not upload an import file

Execution Flow

1. DPOD will check the file size limit, file extensions, and other initial validations.
2. A custom python script will be executed to check and possibly override the deployment policy that was selected by the user.
3. A custom python script will be executed to run validations on the import file (for example - check that the file is not a domain export).
4. If "Dry Run Before" was checked by the user - run a Dry-Run Import.
5. If the Dry Run finished successfully (or was not requested) - perform the actual import.

Reports/Alerts

- Reports
- Reports History
- Alerts
- Alerts History

Reports

The reports view lists all the reports available in the system. DPOD provides some reports out of the box, but you or your administrator may create additional reports to address specific needs.

Reports are generated as MS-Excel spreadsheets, and DPOD is able to email them, save them to the file system, or call a web service to handle the file.

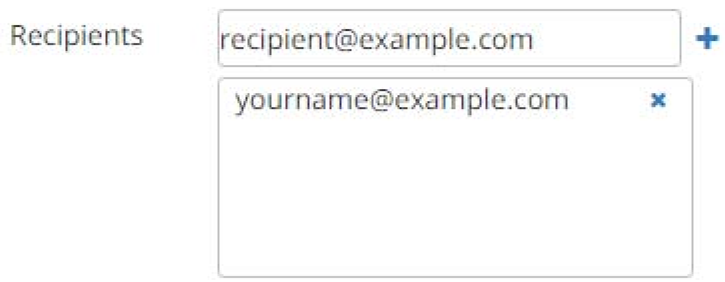
The available reports are displayed in a table with each row describing a single report:

Column Content	Description
Execute Button	Click to execute the report
Name	The name of the report. Click on the name to display the report details and recent execution history
Description	Text description of the report's definition
Schedule	Details of the auto-execution schedule if it exists, or N/A if it doesn't
Recipients	A list of email addresses the report will be emailed to.

EXECUTING A REPORT

To execute a report, click on the Execute button next to its name. This will load the report in the Execute Report screen.

The Execute Report screen allows you to set report-recipients. You may set these by using the Recipients controls:



Recipients

recipient@example.com +

yourname@example.com ✖

The upper box lets you enter an email address of a recipient. Click the + icon to add this recipient to the list inside the lower box.

Click the ✖ icon next to an email address in the lower box to remove them from the list of recipients.

This screen also displays report filters. You may use the filters to control the data generated by the report. The filters available for each report are described in the report's section in this guide.

DPOD will schedule the report to run immediately. When the report is ready, the MS-Excel spreadsheet will be emailed to all the recipients you selected.

SINGLE REPORT VIEW

Clicking on a report name in the table displays the single-report view. This view comprises 2 widgets:

Report Details

Provides the name and description of the report, alongside a list of all configured recipient email addresses. You may click the Execute button found inside this widget to execute the report.

Recent Executions

List the 20 most recent executions of the displayed report. The data is displayed in a table.

Each row in the table provides details of a single report execution.

Column Content	Description
Recipients	A list of email addresses that were sent the report that resulted of this execution

Executing User	The user executing the report
Status	Report Execution status
Status Time	The time this status was set by the system
Message	Message for failed execution

SPREADSHEET DETAILS

When you select to email reports, each recipient receives a copy of a MS-Excel spreadsheet with the content of the report. The first three row of every report contain the following information:

Header	Content
Report Name	The report's name
Execution Time	A timestamp for the report's execution
Executing User	The user that requested the report
Time Range	The value of the time filter used

Reports Setup

Click on "Add Report" to create a new report.
Click on the report name and press "Edit" to enter the alert details page.

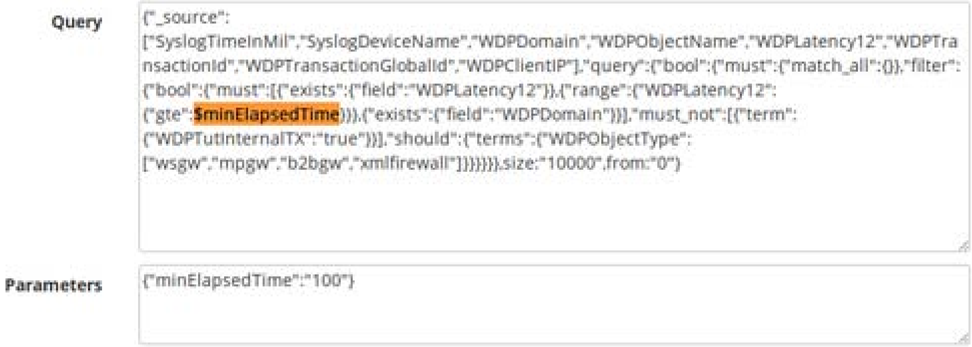
Column	Description
Description	A description of the report
Product	Product Type
REST URL	Report invocation can be integrated with external application via rest api, see Reports REST API from more details.
Schedule	When an alert execution will be scheduled
Recipients	Email addresses of the recipients for the report publishing.

Add / Edit Report

Report Details Section

Field	Description
Name	Name of the report
Description	Description of the report
Product	Product Type
API Reference	A unique key to be used in REST API. See Reports REST API for more details.
Schedule	When the report will be executed. See Scheduling a Report for more details.
Recipients	Email addresses of the recipients for the report publishing

Report Query Section

Field	Description
Index Sets	Which ElasticSearch index sets will be queried (according to product type)
Document Types	Which ElasticSearch document types will be queried (according to product type)
Query (JSON)	An ElasticSearch query
Parameters (JSON)	Named parameters to replace placeholders in the query. i.e:  Query {"_source":["SyslogTimeInMil","SyslogDeviceName","WDPDomain","WDPObjectName","WDPLatency12","WDPTransactionId","WDPTransactionGlobalId","WDPClientIP"],"query":{"bool":{"must":{"match_all":{}},"filter":{"bool":{"must":[{"exists":{"field":"WDPLatency12"}},{"range":{"WDPLatency12":{"gte":$minElapsedTime}}},{"exists":{"field":"WDPDomain"}}],"must_not":[{"term":{"WDPTutInternalTX":"true"}}],"should":{"terms":{"WDPObjectType":["wsgw","mpgw","b2bgw","xmlfirewall"]}}}}}}},size:"10000",from:"0"} Parameters {"minElapsedTime":"100"}
Headers (JSON)	Named parameters to replace column headers in reports outcome with more meaningful headers.

Report Filters Section (according to product type and document type)

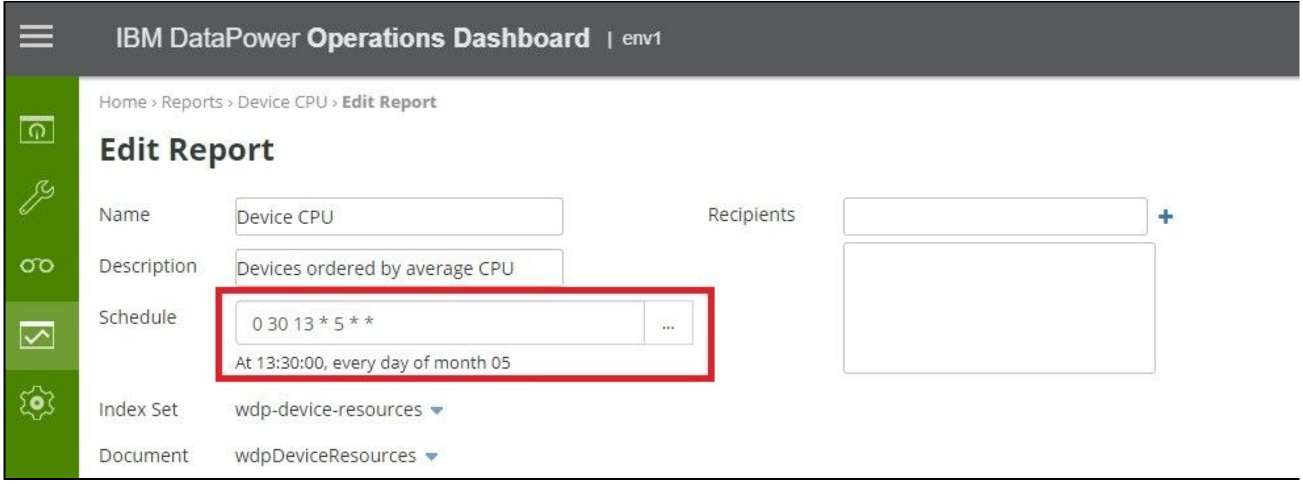
Field	Description	Product Type
Time Range	Time frame for the query to sample the data for the report	Gateway/API-C
Device	Which DataPower devices the alert's query should check	Gateway/API-C
Domain	Which DataPower domains the alert's query should check	Gateway/API-C
Service	Which DataPower services the alert's query should check	Gateway
Service Field Override	Apply the service filter value to a specific Store field. You may leave this field empty unless otherwise advised.	Gateway
Catalog	Which API-C catalog names the alert's query should check	API-C
Space	Which API-C space names the alert's query should check	API-C
Product	Which API-C product names the alert's query should check	API-C
Plan	Which API-C plan names the alert's query should check	API-C
API Name	Which API-C names the alert's query should check	API-C
API Version	Which API-C versions the alert's query should check	API-C
App Name	Which API-C names the alert's query should check	API-C

*By choosing "Adjustable Before Execution", the filter/s will/won't be available in the "Execute Report" page.

Scheduling a Report

The following steps will let you automatically schedule a report.

1. On the Web Console - navigate to the reports page
2. Click on the name of the report you want to schedule
3. Click the "Edit" button at the top-right
4. The "Schedule" input box will contain the scheduling definition using a simplified version of the Cron scheduling format:
   You can input the Cron scheduling expression manually or use the wizard.


IBM DataPower Operations Dashboard | env1
Home › Reports › Device CPU › Edit Report
Edit Report
Recipients
+
...
Index Set
Document

Name: Device CPU

Description: Devices ordered by average CPU

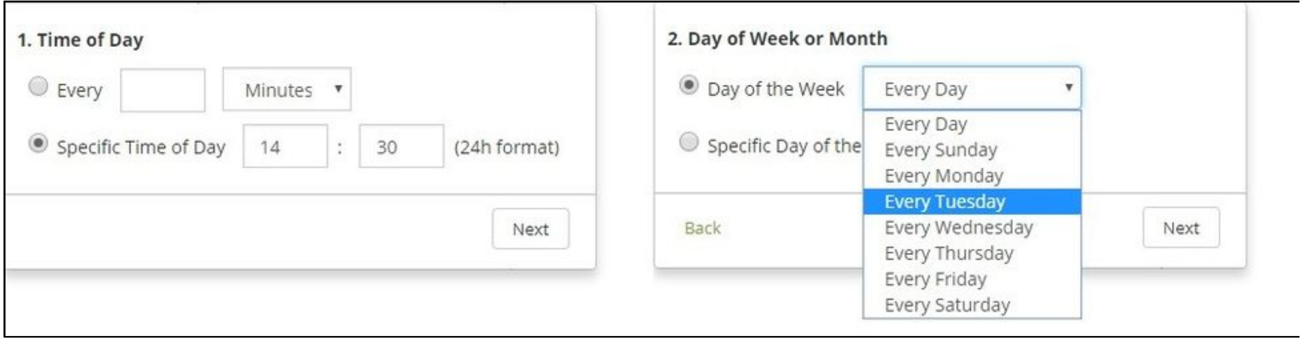
Schedule: 0 30 13 * 5 * *

At 13:30:00, every day of month 05

Index Set: wdp-device-resources

Document: wdpDeviceResources

5. To Use the Wizard, click on the three dots button
   The first window will ask for the time of day - e.g. run every 5 minutes or 10 hours at minute 30, or a specific time of day - e.g. 14:00.
   The second window will ask for the day of week or month - e.g. run every day, every Sunday, or each 5th day of the month.



6. If you need a more sophisticated expression, enter the schedule expression manually in the input field, instead of using the wizard:
   a. The format is "**Second Minute Hour Day Month Weekday Year**"
   b. Separate values with one blank space
   c. Valid values are:
      i. **Second**: 0-59
      ii. **Minute**: 0-59
      iii. **Hour**: 0-23
      iv. **Day**: 1-31
      v. **Month**: 1-12
      vi. **Weekday**: 0-6 (where 0 is Sunday, and 6 is Saturday)
      vii. **Year**: 1000-9999
   d. Multiple values may be specified using the following formats:
      i. ***** : every value (e.g. every second, every minute etc.)
      ii. ***/i** : interval of ***i*** units (e.g. every 5 minutes, every 4 hours)
      iii. **s/i** : interval of ***i*** units starting value **s** (e.g. every 2 hours starting 14 hours)
      iv. **x,y,z** : list of values (e.g. on hours 11,13,15)
   e. **Examples:**
      i. 0 30 7 1 * * *   = run at 07:30:00, 1st day of every month
      ii. 0 30 7,8,9 * * 1 *   = run at 07:30:00, 08:30:00 and 09:30:00, every Monday
      iii. 0 */5 * * * * *   = run every 5 minutes
      iv. 0 0 0 * 5 * *   = run at midnight, every day in May
      v. 0 0 * 1 1 * 2017 = run every hour, on January 1st, 2017
      vi. 0 55/1 * * * * *   = run on minutes 55, 56, 57, 58, 59 of every hour
   f. When you have entered a schedule value, move to another input field (e.g. press tab), and a message with human readable description of the scheduling will be displayed underneath the input box
   g. Click "Update" to save your changes

List of Built in Reports

- API Latency Report
- Device CPU Report
- Device Resources Report
- Domain Request Size Report
- Domain Total Transactions Report
- Executed Transactions Report
- Message Codes Count Report
- Service Average Latency Report
- Service Average Request Size
- Service Elapsed Time Report
- Service List Report
- Service Memory Report
- Service Total Errors Report
- Service Total Successful Transactions Report
- Service Total Transactions Report
- System Errors Report
- Total API Executions Report
- Transactions Above Elapsed Time
- URI Detailed Latency Report
- URI Summary Latency Report

API LATENCY REPORT

API Latency

Available Filters

- Time Range
- Device
- Domain
- Catalog
- Space
- Product
- Plan
- API Name
- API Version
- App Name

Summary Table

Column	Description
Key	The catalog name
doc_count	Number of times the catalog name appeared for the specified filters (time, device, etc)
Key	The API Name
doc_count	Number of times the API name appeared for the catalog name
Key	The API Version
doc_count	Number of times the API version appeared for the api name
Key	The FE Response code
doc_count	Number of times the FE Response code appeared for the api version
Key	Average Total Latency
doc_count	Average total latency for each response code
Key	Max Total Latency
doc_count	Max total latency for each response code

Default Sort: First doc_count, Descending.

DEVICE CPU REPORT

Devices ordered by average CPU

Available Filters

- Time Range
- Device

Summary Table

Column	Description
Device	The device name
Samples	Samples recorded for the device
Average CPU (%)	Average CPU utilization recorded across samples
Maximum CPU (%)	Maximum CPU utilization recorded across samples

Default Sort: Average CPU (%), Descending.

DEVICE RESOURCES REPORT

All device resources samples

*The Device Resources report will return up to 10,000 rows

Available Filters

- Time Range
- Device

Summary Table

Column	Description
Total Installed Memory	Total installed memory in the monitored device
Used Memory (%)	Used memory (Percent)
Sample Time	Sample time
System Load	System load percentage
Used CPU (%)	Used CPU percentage
Device Name	The device where the sample run

Default Sort: Sample Time, Ascending.

DOMAIN REQUEST SIZE REPORT

Domains ordered by total request size

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Domain	The domain name
Transactions	Number of transactions for the domain
Total Request Size (bytes)	Total size of messages for the domain

Default Sort: Total Request Size (bytes), Descending.

DOMAIN TOTAL TRANSACTIONS REPORT

Domains ordered by total number of transactions

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Domain	The domain name
Transactions	Number of transactions for the domain

Default Sort: Transactions, Descending.

EXECUTED TRANSACTIONS REPORT

List of all executed transactions

Available Filters

- Time Range
- Device
- Domain
- Service

Summary Table

Column	Description
Time	Transaction execution time
Transaction ID	The transaction id
Client IP	The client IP of the machine (or load balancer) where this transaction started
Device	The device where the transaction run
Domain	The domain where the transaction run
Service Name	Service name

Default Sort: Time, Descending.

MESSAGE CODES COUNT REPORT

Message codes distribution

Available Filters

- Time Range
- Device
- Domain
- Service

Summary Table

Column	Description
Key	The message code (for example 0x80e0068d)
doc_count	Number of times the message code appeared for the specified filters (time, device, etc)
Key	Message Log level
doc_count	Number of times the message code appeared for the log level

*There may be one or more log levels where the message appeared, each log level will be shown in the separate line.

Default Sort: First doc_count, Descending.

SERVICE AVERAGE LATENCY REPORT

Average latency report per services

Available Filters

- Time Range
- Device
- Domain
- Service

Summary Table

Column	Description
Service Name	Service name
Executions	Number of service executions within time range.
Avg Front-End Request - Network Latency (ms.)	Average front-end request network latency in milliseconds.
Avg Front-End Response - Network Latency (ms.)	Average front-end response network latency in milliseconds.
Avg Gateway Response Latency (ms.)	Average gateway response network latency in milliseconds.
Avg Service Elapsed Time (ms.)	Average elapsed time in milliseconds in milliseconds.
Avg Back-End Request - Network Latency (ms.)	Average back-end request network latency in milliseconds.
Avg Gateway Request Latency (ms.)	Average gateway request network latency in milliseconds.
Avg Back-End Response - Network Latency (ms.)	Average back-end response network latency in milliseconds.
Avg Backend Elapsed (ms.)	Average back-end elapsed network latency in milliseconds.

Default Sort: Avg Service Elapsed Time (ms.), Descending.

SERVICE AVERAGE REQUEST SIZE

Average request size per service

Available Filters

- Time Range
- Device
- Domain
- Service

Summary Table

Column	Description
Service Name	Service name
Executions	Number of service executions within time range.
Average Request Size (bytes)	Average request size in bytes.

Default Sort: Average Request Size (bytes), Descending.

SERVICE ELAPSED TIME REPORT

Services ordered by average elapsed time

Available Filters

- Time Range
- Device

- Domain

Summary Table

Column	Description
Service	Service name
Transactions	Number of transactions for the service
Average Time (ms)	Average elapsed time across all samples
Maximum Time (ms)	Maximum elapsed time across all samples

Default Sort: Average Time (ms), Descending.

SERVICE LIST REPORT

Detailed Service List

> This report will produce output only when DPOD's service configuration sampling is enabled (it is enabled by default)

Available Filters

- Time Range
- Device

Summary Table

Column	Description
FE Request Queue	Front end Request Queue
BE Request Queue	Back end Request Queue
FE Service Name	Front end service name
FE Protocol	Front end protocol this service runs on.
FE Port	Front end TCP port for this service
BE Qmgr Name	Back end Queue Manager for this service (when relevant)
FE URI	Front end URI for this service
FE Address	Front end IP Address for this service.
Domain	The domain this service is deployed on
FE Qmgr Name	Front end Queue Manager for this service (when relevant)
Device	The device this service is deployed on
BE Response to Queue	Front end Response Queue
Service Name	The service name
FE SOAP version	SOAP Version for this service (where applicable)
BE Protocol	Back end protocol this service runs on.
FE Response to Queue	Front end Response Queue
BE URI	Back end URI for this service
BE Service Type	Back end type of service. (for example, MultiProtocolGateway, XMLFirewallService, etc)
BE Port	Back end TCP port for this service
FE QMGR Group	Front end Queue Manager Group for this service (when relevant)

BE Address	Back end IP Address for this service

SERVICE MEMORY REPORT

Services ordered by average consumed memory

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Service	Service name
Samples	Number of samples for the service
Average Memory (KB)	Average memory utilization across all samples
Maximum Memory (KB)	Maximum memory utilization across all samples

Default Sort: Average Memory (KB), Descending.

SERVICE TOTAL ERRORS REPORT

Services ordered by total number of erroneous transactions

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Device	Device name
Service	Service name
Errors	Total number of errors for the service in domain

Default Sort: Errors, Descending.

SERVICE TOTAL SUCCESSFUL TRANSACTIONS REPORT

Services ordered by total number of successful transactions

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Service	Service name
Successful Transactions	Total number of successful transactions for the service

Default Sort: Successful Transactions, Descending.

SERVICE TOTAL TRANSACTIONS REPORT

Services ordered by total number of transactions

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Service	Service name
Transactions	Total number of transactions for the service

Default Sort: Transactions, Descending.

SYSTEM ERRORS REPORT

Critical system error messages

Available Filters

- Time Range
- Device

Summary Table

Column	Description
Message	The error message key
Count	The number of errors encountered for this message-key

Default Sort: Count, Descending.

Error Details Table

Column	Description
Message	Message text
Time	The timestamp (to milliseconds) the error was recorded at
Severity	Severity of the error. Valid Values: • error • critic
Device	The name of the device where the error was found
Category	WDP category of the message

Default Sort: Time, Descending.

TOTAL API EXECUTIONS REPORT

Total API Executions

Available Filters

- Time Range
- Device
- Domain
- Catalog
- Space
- Product
- Plan
- API Name

- API Version
- App Name

Summary Table

Column	Description
Key	The catalog name
doc_count	Number of times the catalog name appeared for the specified filters (time, device, etc)
Key	The API Name
doc_count	Number of times the API name appeared for the catalog name
Key	The API Version
doc_count	Number of times the API version appeared for the api name
Key	The FE Response code
doc_count	Number of times the FE Response code appeared for the api version

Default Sort: First doc_count, Descending.

TRANSACTIONS ABOVE ELAPSED TIME

Transactions with elapsed time greater or equals to a threshold

Available Filters

- Time Range
- Device
- Domain
- Service

Summary Table

Column	Description
Elapsed (ms.)	The elapsed time in milliseconds of the transaction
Time	Transaction execution time
Transaction ID	Transaction id
Client IP	The client IP of the machine (or load balancer) where this transaction started
Device Name	Device executing the transaction
Global Transaction ID	Global transaction id
Domain Name	The domain on the device

Default Sort: Average Request Size (bytes), Descending.

URI DETAILED LATENCY REPORT

Detailed URI Latency Report

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
Elapsed Time (ms)	The elapsed time in milliseconds of the transaction

Device	The device where the transaction Run
Service URI	URI of the transaction
Domain	The domain where the transaction Run

URI SUMMARY LATENCY REPORT

URI Request Summary Latency List

Available Filters

- Time Range
- Device
- Domain

Summary Table

Column	Description
URI	URI of the transaction
Total Transactions	How many transactions run during the time for this URI
90% Percentile(ms)	The latency in ms. of the 90% percentile of transactions for this URI
95% Percentile(ms)	The latency in ms. of the 95% percentile of transactions for this URI
99% Percentile(ms)	The latency in ms. of the 99% percentile of transactions for this URI
Average Time (ms)	The latency average in ms. of all transactions for this URI
Minimum Time (ms)	The latency in ms. of the transaction with the minimum latency for this URI
Maximum time(ms)	The latency in ms. of the transaction with the maximum latency for this URI

Default Sort: Average Time (ms), Descending.

Reports History

The reports history page shows log of all recent report executions (limited by storage), and allows to download the report output for 30 days after the execution.

Column	Description
Name	The report's name
Recipients	A list of email addresses the report will be emailed to.
Executing User	The user executing the report
Status	Report Execution status
Status Time	The time this status was set by the system
Message	Message for failed execution
Download	If an output file exists for the report, the user can download the report. Report output is automatically deleted after 30 days.

Alerts

DPOD can publish alerts when certain predefined events occur, for example, when device CPU is over 80%
Alerts can be viewed and managed from the Alerts Setup page

TERMINOLOGY

Alert Query - the metadata that defines the alert parameters (for example, count all the system errors from the last 10 minutes in domain DMZ)

Alert Execution - one execution of the alert query

Alert Publishing - when an alert returns positive results, it will be published to interested parties via email or syslog

ALERT QUERY

Each query consists of a type, period, an operator and a threshold.
In addition, you can define filters, so the query will run on specific devices, domains or services.

DPOD supports 4 types of alerts queries:

Type	Description	Example
Frequency	The condition will be met if there were X events in the checked time	More than 5 system errors occurred in the last 10 minutes
Flatline	The condition will be met if there is a value above a certain threshold	Device CPU is above 80%
Any	The condition will be met if any results are returned for the query	A DataPower object is down
List	The condition will be met if a result is in/not-in a pre-defined list of values	

ALERT EXECUTION

An execution is one instance of the alert query, there are 3 ways to execute a query:

1. **Scheduled** - Enabled queries can be scheduled to run on a specific time or on a fixed interval.
2. **Test Via the web console** - Click the "Test" button in the Alerts Details Page for a one time only execution, you can use it for testing the query before scheduling it.
3. **Via the REST API** - an alert can be executed remotely via the REST API (for example, with CURL), the REST API URL for each query can be found in the Alerts Details Page, Example can found here

ALERT PUBLISHING

The alert will be published once an alert execution run an alert query and generated one or more results.

The alerts can be published via the following facilities:

- **Email** (or **Email WS**) - an email will be sent for every generated alert.
  Make sure that "Enable Queries Emails SMTP" (or "Enable Queries Emails SMTP WS") is set to true in the System Parameters page.
  For further details about the format of the email message see Alerts Email Format.
- **Syslog message** - a Syslog message will be sent for every generated alert.
  The Syslog target server's host name, port and the syslog severity field value (Error, Info, etc.) can be configured in the System Parameters page.
  For further details about the format of the Syslog message see Alerts Syslog Format.

Alerts Setup

The Setup Alerts page shows details about existing system alerts, and lets you edit them and create new alerts.

Click on "Add Alert" to create a new alert.
Click on the alert name to enter the "alert details" page and edit the alert.

Column	Description
Enabled	Shows whether or not the alert execution will be scheduled to run (this is a read only field, you can change it by editing the alert)
Name	The alert's name, click on the name to go to the Alert details Page - you can edit the alert from there.
Description	A description of the alert - displays the "Query Value" field of the alert
Schedule	When an alert execution will be scheduled - The alert will not be scheduled if it is not enabled, even if this field contains a value
Recipients	"Syslog" and/or the email addresses of the recipients for the alert publishing

Alert Details page

The top part displays the following fields:

Field	Description
Enabled	Whether or not the alert will be scheduled for execution
System Health Metric	Whether or not the alert is a metric
Description	A description of the alert -displays the value of the "Query Value" field of the alert
Product	Product Type
Schedule	When an alert execution will be scheduled (if the alert is not enabled the alert will not be scheduled)
REST URL	The URL to run the alert via REST
Recipients	"Syslog" and/or the email addresses of the recipients for the alert publishing

The top part of the page also contains three buttons:
Test - Execute the alert immediately, the alert will be executed **even if it's disabled**, this is helpful in case you want to check the alert before actually scheduling it.
Edit - Edit the alert
Delete - Delete the alert

> Deleted alert cannot be recovered.
> If you simply do not want the alert to run - you can disable it (press "Edit" and uncheck the "Enabled" field)

The lower part of the page displays the results of the recent 20 executions of the alert

Field	Description
Executing User	SCHEDULER - if DPOD run an alert execution via the scheduler REST - if the alert was run via the REST API User name - if a user tested the alert by pressing the "Test" button
Status	The execution status
Status Time	When the status was set
Message	How many alerts were generated (or an error message if a problem occurred)

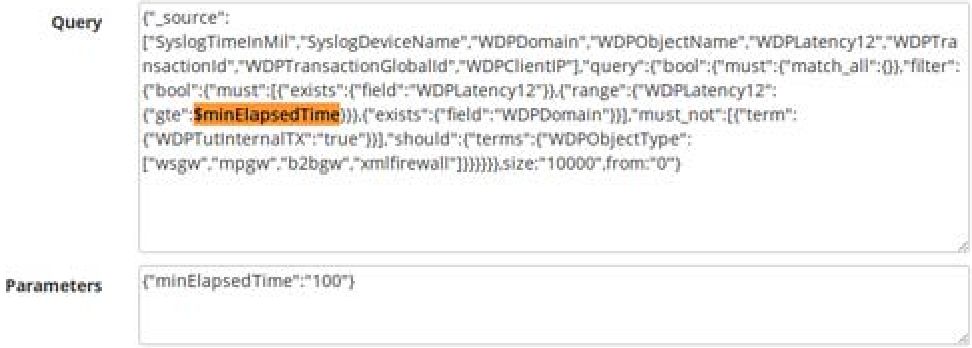
Add / Edit Alert

The first section contains details about the execution of the alert

Field	Description
Enabled	Whether or not the alert will be scheduled for execution
System Health Metric	Whether or not the alert is a metric
Name	The Alert's name
Product	Gateway or API-C
Schedule	When the alert will be scheduled, the format is identical to the one used to schedule reports
Destination	Specify the alert publishing destinations: **Syslog** - a syslog record will be written, you'll need to configure the Syslog target server's host name, port and the syslog severity field value (Error, Info, etc) in the System Parameters page. **Email** - send an email (make sure that "Enable Queries Emails SMTP" is set to true in the System Parameters page) **Email WS** - send an email via webservice (make sure that "Enable Queries Emails SMTP WS" is set to true in the System Parameters page)
Recipients	if the destination is Email or Email WS - this field will contain the list of recipients

The Alert Details section contains information about how the alert's query will be evaluated

Field	Description
Type	The alert type (more information about the alert types can be found in the the Alerts page)
Query Value	Free text, describes the results returned by the alert's query **Press the "Details" button to view the alert query itself**
Index Sets	(Hidden by default) Which ElasticSearch index sets will be queried
Document Types	(Hidden by default) Which ElasticSearch document types will be queried
Query (JSON)	(Hidden by default) An ElasticSearch query

Parameters (JSON)	(Hidden by default) Named parameters to replace placeholders in the query. i.e:
	
	Query
	`{"_source":["SyslogTimeInMil","SyslogDeviceName","WDPDomain","WDPObjectName","WDPLatency12","WDPTransactionId","WDPTransactionGlobalId","WDPClientIP"],"query":{"bool":{"must":{"match_all":{}},"filter":{"bool":{"must":[{"exists":{"field":"WDPLatency12"}},{"range":{"WDPLatency12":{"gte":$minElapsedTime}}},{"exists":{"field":"WDPDomain"}}],"must_not":[{"term":{"WDPTutInternalTX":"true"}}],"should":{"terms":{"WDPObjectType":["wsgw","mpgw","b2bgw","xmlfirewall"]}}}}}},size:"10000",from:"0"}`
	Parameters
	`{"minElapsedTime":"100"}`

Query Period	The time frame for the alert's query
Operator	Operator for the alert's query

Threshold	The value to compare the query's result to (not applicable for alert types "any" and "list" Border
Field Name	Only applicable for alert type "list"
Value List	Only applicable for alert type "list" - the list of values delimited by the delimiter specified in the "delimiter" field

The Alert Filters section lets you specify additional criteria for the alert's query according to the product type and document type

Field	Description	Applicable Product Type
Device	Which DataPower devices the alert's query should check	Gateway/API-C
Domain	Which DataPower domains the alert's query should check	Gateway/API-C
Service	Which DataPower services the alert's query should check	Gateway
Catalog	Which API-C catalog names the alert's query should check	API-C
Space	Which API-C space names the alert's query should check	API-C
Product	Which API-C product names the alert's query should check	API-C
Plan	Which API-C plan names the alert's query should check	API-C
API Name	Which API-C names the alert's query should check	API-C
API Version	Which API-C versions the alert's query should check	API-C
App Name	Which API-C names the alert's query should check	API-C

List of Built in Alerts

Alerts

Name	Type	Description
About to Expire Certificates Alert	Gateway	Alert for certificates that are about to expire. The alert will check for syslog message with code 0x806000e2 that were written in the last 24 hours
Already Expired Certificates Alert	Gateway	Alert for certificates that already expired - the alert will check for syslog messages with code 0x806000e1 that were written in the last 24 hours
Domain Restarts Alert	Gateway	Alert on domain restarts
Message Codes Frequency Alert	Gateway	Alert when message codes frequency exceeds threshold value
Number of Probes Alert	Gateway	Alert if more than 1000 transactions with probles were run in the last 10 minutes
Objects Down Alert	Gateway	Alert on all the DataPower objects that are enabled in configuration but in a down state (similar to the data shown in the Failed Objects page)
Syslog Errors MessageCode Alert	Gateway	Alert when a specific syslog message is written (only messages with severity = error) You will need to edit this alert and enter the message codes to alert on instead of the supplied sample message code (0x81000098)
Transaction Errors Alert	Gateway	Alert when 5 or more transactions with errors ran in the last 30 minutes Please note: When duplicating this alert - the new alert name must start with "Transaction_Errors" (e.g. "Transaction_Errors_2")
Unused Services	Gateway	Alert when service total transactions equals to zero
API Latency Above 100ms Alert	API-C	Alert if more than 5 API Connect API calls finished with latency of over 100ms Change 5 to any other number using the field "Error Threshold" To change "100" to any other latency, you will need to edit the JSON - duplicate the alert first, as system predefined alerts' JSON cannot be edited
APIs That Ended in Error Code Range	API-C	Alert on any API transaction that ended with status code 500. You may change the range of the status code by editing the parameters JSON (for example, alert on statusCode between 300 and 600)

System Health Metrics

See System Health for more detailes

Name	Description
Devices CPU Metric [1]	Alert when the max device CPU during the last 5 minutes was over 80%
Devices Fan Metric [1]	Alert when the device fan health is less than 100%
Devices Load Metric [1]	Alert when the max device load in the last 5 minutes was more than 80%
Devices Memory Metric [1]	Alert when the max used memory of the device in the last 5 minutes was over 70%
Devices Space Encrypted Metric [1]	Alert if the free space of the encrypted file system is less than 15%
Devices Space Internal Metric [1]	Alert if the free space of the internal file system is less than 15%
Devices Space Temp Metric [1]	Alert if the free space of the temporary file system is less than 15%
Devices Temperature Metric [1]	Alert when the device temperature health is less than 100%
Devices Voltage Metric [1]	Alert if the device's voltage health is less than 100%
System Errors Metric	Alert if more than 10 critical system errors were written to syslog in the last 5 minutes

(1) The following alerts and metrics are valid only for devices with the option "Device Resources Monitoring" enabled. You may edit the device setting from [Manage Devices Monitored Devices].
See also Adding Monitored Devices.

Alerts Syslog Format

Syslog Format for Flatline/ Frequency alerts

Name	Example	Description
Syslog facility code	<16>	Always <16>
Time	Oct 23 15:40:43	Alert's execution time
DPOD server host name	dpod	The host name of DPOD server that generated the alert
Alerts Syslog Message ID	[0x00a0001a]	Always [0x00a0001a]
Category	[DPOD-alert]	Always [DPOD-alert]
Severity Level	[info]	May be set via System Parameters ("Syslog Severity Field Value")
Alert Name	AlertName:(Devices CPU Metric)	The alert name as defined in Alerts Setup
Alert Description	AlertDesc:(Alert on Devices CPU over 80%)	The alert description as defined in Alerts Setup
Alerted Object	on:(idg77)	The object (device, service, message, etc.) the alert was generated on
Alert Value	Value:(85.0)	The query's result value
Alert Threshold	Threshold:(75.0)	The alert error threshold as defined in Alerts Setup
Alert Filters	Filters:[device(),domain(),service()]	Additional criteria for the alert's execution
Time Range	Interval:[timestampStart(10/23/2018 15:35:43.714),timestampStartLong(1540298143714), timestampEnd(10/23/2018 15:40:43.714),timestampEndLong(1540298443714)]	The time frame for the alert's execution

Syslog Format for Any/ List alerts

Name	Example	Description
Syslog facility code	<16>	Always <16>
Time	Oct 24 08:30:23	Alert's execution time
DPOD server host name	dpod	The host name of DPOD server that generated the alert
Alerts Syslog Message ID	[0x00a0001a]	Always [0x00a0001a]
Category	[DPOD-alert]	Always [DPOD-alert]
Severity Level	[info]	May be set via System Parameters ("Syslog Severity Field Value")
Alert Name	AlertName:(Objects Down Alert)	The alert name as defined in Alerts Setup
Alert Description	AlertDesc:(Alert on any DP object that is enabled but down)	The alert description as defined in Alerts Setup
Alerted Object	on:([Domain is down, LogTarget, idg77, HospitalA_Domain])	The object (device, service, message, etc.) the alert was generated on

Alert Value	Value:(null)	The alert value is not applicable for alert types "any" and "list"
Alert Threshold	Threshold:(null)	The alert threshold is not applicable for alert types "any" and "list"
Alert Filters	Filters:[device(),domain(),service()]	Additional criteria for the alert's execution
Time Range	Interval:[timestampStart(10/24/2018 08:25:23.531),timestampStartLong(1540358723531), timestampEnd(10/24/2018 08:30:23.531),timestampEndLong(1540359023531)]	The time frame for the alert's execution

Alerts Email Format

Email Subject

The subject consists of a permanent prefix "DPOD_MSC Alert - " and the alert name as defined in Alerts Setup.

Email Body

Hello,
The following alert was generated by DPOD: Alert on Devices Memory over 70%
Alert on xi750, value 30.0
Alert on idg72, value 29.0
Alert on xg751, value 27.0
Alert Parameters:
Name: Devices Memory Metric
Threshold: 20.0
JSON Parameters: n/a
Filters: device: n/a ,domain: n/a ,service: n/a
Time Range: From 10/23/2018 16:55:38 (1540302938172) To 10/23/2018 17:00:38 (1540303238172)
This email has been sent to you by DPOD_MSC Alerts Server. Please do not reply to this email.

Email Part	Example	Description
Hello,		Permanent title
The following alert was generated by DPOD:	Alert on Devices Memory over 70%	The alert description as defined in Alerts Setup
Alerted Objects	Alert on xi750, value 30.0 Alert on idg72, value 29.0 Alert on xg751, value 27.0	Each alerted object will have a line describing the alert details, including the object name and the alert query's result value
Alert Parameters:		Permanent title
Name:	Devices Memory Metric	The alert name as defined in Alerts Setup
Threshold:	20.0	The alert error threshold as defined in Alerts Setup
JSON Parameters:	n/a	The alert named parameters as defined in Alerts Setup
Filters:	device: n/a ,domain: n/a ,service: n/a	Additional criteria for the alert's execution
Time Range:	From 10/23/2018 16:55:38 (1540302938172) To 10/23/2018 17:00:38 (1540303238172)	The time frame for the alert's execution
This email has been sent to you by DPOD_MSC Alerts Server. Please do not reply to this email.		Permanent message

Alerts History

The alerts history page shows log of all recent alert executions (limited by storage), and allows to download any alerts that were produced as JSON files.
The alert JSON files are deleted after 30 days.

Column	Description
Name	The alert's name
Executing User	SCHEDULER - if DPOD run an alert execution via the scheduler REST - if the alert was run via the REST API User name - if a user tested the alert by pressing the "Test" button
Status	The execution status
Status Time	When the status was set
Message	How many alerts were generated (or an error message if a problem occurred)
Download	If an output file exists for the alert, the user can download the result The alert JSON files are deleted after 30 days.

Admin Guide

Intended Audience

The IBM DataPower Operations Dashboard (DPOD) admin guide is intended to be used by DataPower administrators setting up and maintaining DPOD.

The information in the guide is split into the following sections

- Installation and Upgrade
- Uninstall
- Management and Configuration
- DevOps Portal Setup and Security
- Appliance Maintenance
- Security
- High Availability, Resiliency or Disaster Recovery
- Troubleshoot
- Considerations for GDPR readiness

Installation and Upgrade

This section provides a walk-through the process of installing or upgrading a DPOD instance.

Planning for Installation

The following pages describe the pre-installation steps required to accomplish a smooth installation of DPOD.

- Hardware and Software Requirements
- Prepare pre-installed Operating System
- Network Preparation
- Prepare your Monitored Devices

Installation Process

The following pages describe the installation process for IBM DataPower Operations Dashboard.

- Appliance Installation
- Software Deployment
- Installation Verification

Post Installation Steps

The following pages describe steps normally performed immediately post installation.

- Adding Monitored Devices
- Configuring Reports by Email

Planning

These are the preparation steps required to accomplish smooth installation of DPOD.

- Installation Scenarios
- Hardware and Software Requirements
- Network Preparation
- Prepare Pre-Installed Operating System
- Prepare your Monitored Devices

Installation Scenarios

DPOD's packaging options support different scenarios:

1. **Appliance Mode** - Installation on a virtual/physical server
    a. Choose Editions - Developer or Standard
    b. Download ISO file
    c. Verify your system requirements , choose a load type and make sure you can allocate the needed resources
    d. Prepare your network configuration
    e. Prepare your monitored devices
    f. Perform the Appliance Installation path
    g. Verify your installation
    h. Consider do the post installation steps

2. **Non Appliance Mode** Installation on a Pre-installed server (physical/virtual) with CentOS /RHEL 7.2 only
    a. Verify your system requirements and choose a load type and make sure you can allocate the needed resources
    b. Verify your network configuration requirements
    c. Verify your monitored devices requirements
    d. Prepare the Pre-installed OS for DPOD installation.
    e. Download CEF packaging (Compressed Executable File)
    f. Perform the Non-Appliance Installation path
    g. Verify your installation
    h. Consider do the post installation steps

3. **Developer Edition** Installation is used for developer use only and aim to be installed on Laptops.
    a. Chose deployment options : ISO file to install on VM Player or Workstation.
    b. Verify your system requirements , choose a load type and make sure you can allocate the needed resources
    c. Prepare your network configuration
    d. Prepare your monitored devices
    e. For ISO installation - read this .
    f. Verify your installation

4. **Multi Node Federation deployment** - Installation on a virtual/physical server
    a. Submit a sizing request to IBM L2. All Multi node installation will require finalize sizing process to be supported for performance aspects.
    b. Download ISO file and CEF file.
    c. review instructions of a cell environment installation and follow network requirements.
    d. Manager installation - Perform an installation of **Appliance Mode** or **Non-Appliance Mode** with **Medium Load** architecture type to be used as a Manager of the Nodes (Cell Member) in the Cell.
    e. Cell Member installation - Perform an installation of **Appliance Mode** with **High_20dv Load** architecture type to to add a single Cell Member to cell
    f. Cell Member Federation - follow the steps for a Cell Member federation.
    g. Prepare your monitored devices
    h. Perform the Appliance Installation path
    i. Verify your installation
    j. Consider do the post installation steps

DEVELOPER EDITION

The Developer Edition's (previously known as Light Edition) aim is to assist the developer, administrator and technical presale staff to evaluate the product on a workstation environment.

It is geared towards the DataPower developer that wants to run DPOD on their development workstation, in the context of **limited** functionality Proof Of Concept.

The Developer Edition should NOT be used for customer POCs. For customer POCs it is recommended to use at least the Standard Edition with minimum configuration load type.

The Developer Edition does not support any upgrades. Each new version requires a full reinstall of the product.

What are the major differences?

The Developer Edition is identical to the GA Edition and has all of its components. It differs in the following aspects:

- Less hardware & software requirements
- Limited configuration
- One extra post-installation step

How to Identify a Developer Edition installation?

The following can be used to identify a Developer Edition:

- The ISO filename should be DPOD-**Developer-CentOS-**<version>.iso and can be downloaded from Fix Central.
- The CentOS installation screen will show Developer Edition.
- A single configuration setup for development that **exists only in the Development ISO file.**

Less Hardware and Software Requirements

Please view the product Hardware and Software requirements that include the Developer Edition's requirements.

Limitations

Developer Edition installations are limited to 10 monitored devices.
Developer Edition installations are limited to 90 days. After 90 days, you will be redirected to a license page where a license request key can be generated.
Send the license request key to an IBM representative to get your license (the representative's email address will appear on screen).

The Developer Edition allows only limited configuration. This means:

- A single type of architecture configuration file that provides a single DPOD node architecture
- 1 WS-M agent
- 1 Syslog agent
- Limited amount of data collected
- No support for upgrades / fixpacks

Docker container for Light Developer edition

For developer usage only, there is a Docker container packaging the allows faster deployment with minimum resources to run on laptops or to demonstrate basic functionalities of DPOD. Please read more here.

Docker Container for Light Developer Edition

The Docker Container for Light Developer Edition is a lightweight Developer Edition (previously known as Light Edition) designated mainly for developers.
It is geared towards the DataPower developer that wants to run DPOD on their development workstation, in the context of **limited** functionality.
The Docker Container for Light Developer Edition does not support upgrades and not entitled to IBM support. Each new version requires deployment of new container.

Limitations

Docker installations are limited to 3 monitored devices.
Docker installations are limited to 7 days. After 7 days, you will be redirected to a license page where a license request key can be generated.
Send the license request key to an IBM representative to get your license (the representative's email address will appear on screen).

Software and Hardware Prerequisites

Software

The Docker Container for Light Developer Edition has been tested only on:

- CentOS 7.4 (kernel 3.10) with Docker CE (Community Edition) version 17.09.1
- Ubuntu 18.04.LTS Desktop with Docker CE version 18.09.2

> Ubuntu Server is not supported, please use Ubuntu Desktop.

- Apple MacOS 10.13.4 with Docker CE version 18.03.1
- Docker on Windows is not supported

> Make sure to configure your Docker installation as recommended in Docker Compatibility Matrix, especially make sure to use the recommended storage driver.

Hardware

1. At least 4GB of disk space that can grow up to 6GB.
2. At least 3GB of free memory.
3. At least 4 Cores of Intel based CPUs.

Installation

Image Download and Installation

Download the desired DPOD Docker image from IBM Docker Hub or from IBM's Fix Central

1. Specific version: datapower-operations-dashboard**:**<version number>. For example: datapower-operations-dashboard:1.0.9.0
2. Latest version: **datapower-operations-dashboard:latest**

Image Installation

There are two options for installing DPOD Docker image on you local image repository:

1. Use the Docker pull command:

```
docker pull ibmcom/datapower-operations-dashboard:latest
```

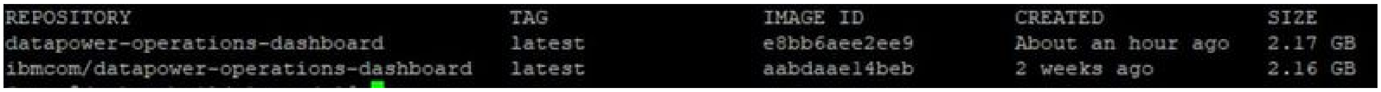
2. Manual load: after downloading the desired images to your Docker host use the load command:

```
docker load < /tmp/DPOD-Developer-Docker-1.0.9.tgz
```

Use the following command to display your local image repository:

```
docker images
```

This is how the result should look like:



```
REPOSITORY                              TAG          IMAGE ID       CREATED             SIZE
datapower-operations-dashboard          latest       e8bb6aee2ee9   About an hour ago   2.17 GB
ibmcom/datapower-operations-dashboard   latest       aabdaae14beb   2 weeks ago         2.16 GB
```

Enable Firewall Rules (CentOS/Ubuntu only)

If needed enable firewall rules for allowing DataPower access to DPOD Docker container agents (syslog on port 60000 and wsm on port 60020) :

```
sudo iptables -I INPUT 1 -p tcp -m tcp -s 0.0.0.0/0 -d 0.0.0.0/0 --dport
60000 -j ACCEPT
sudo iptables -I INPUT 1 -p tcp -m tcp -s 0.0.0.0/0 -d 0.0.0.0/0 --dport
60020 -j ACCEPT
```

save the configuration :

```
sudo iptables-save
```

Create a new Docker container

Use the following command to create a DPOD Docker container:

> Make sure to replace **DPOD_EXT_HOST_IP** parameter value (currently provided as "**<Host IP Address>**") in the command below with the IP Address of the host machine that runs the Docker containers.

```
docker run -d \
   --security-opt seccomp:unconfined \
   --cap-add SYS_ADMIN \
   --cap-add SYS_RESOURCE \
   --cap-add SYS_TIME \
   --tmpfs /tmp:exec \
   --tmpfs /run \
   --tmpfs /run/lock \
   -v /sys/fs/cgroup:/sys/fs/cgroup:ro \
   -v /etc/localtime:/etc/localtime:ro \
   --device /dev/rtc \
   -p 9022:22 \
   -p 443:443 \
   -p 60000:60000 \
   -p 60020:60020 \
   --stop-timeout 10 \
   --hostname dpod \
   --name dpod \
   datapower-operations-dashboard:latest && docker exec -d -u root dpod
/bin/su - -c "export ACCEPT_LICENSE=true; export
TIME_ZONE=America/New_York; export DPOD_EXT_HOST_IP=<Host IP Address>;
/app/scripts/app-init.sh"
```

Notes:

Ports: the container should expose the following ports:

- 22 – SSH access to the container
- 443 – Web Console access
- 60000 – Syslog agent. It is important that you map this port as it is exposed (60000)
- 60020 – WS-M agent. It is important that you map this port as it is exposed (60200)

Special Considerations for Apple MacOS

- The file **/etc/localtime** should be shared with the container: copy the file located on /etc/localtime to the user directory usually located at /Users/<user name>.

  If you choose to copy the file to another directory make sure to add it to the Docker File Sharing (Docker preferences 🐳 -> Preferences -> File sharing).

Example of Docker run command for MacOS:

Make sure to replace **DPOD_EXT_HOST_IP** parameter value (currently provided as "**<Host IP Address>**") in the command below with the IP Address of the host machine that runs the Docker containers.

Make sure to replace <**User Directory>** in the command bellow with the full path of the directory that /etc/localtime was copied to.

```
docker run -d \
   --security-opt seccomp:unconfined \
   --cap-add SYS_ADMIN \
   --cap-add SYS_RESOURCE \
   --cap-add SYS_TIME \
   --tmpfs /tmp:exec \
   --tmpfs /run \
   --tmpfs /run/lock \
   -v <User Directory>/localtime:/etc/localtime:ro \
   -v /sys/fs/cgroup:/sys/fs/cgroup:ro \
   --device /dev \
   -p 9022:22 \
   -p 443:443 \
   -p 60000:60000 \
   -p 60020:60020 \
   --stop-timeout 10 \
   --hostname dpod \
   --name dpod \
   datapower-operations-dashboard:latest && docker exec -d -u root dpod
/bin/su - -c "export ACCEPT_LICENSE=true; export
TIME_ZONE=America/New_York; export DPOD_EXT_HOST_IP=<Host IP Address>;
/app/scripts/app-init.sh"
```

Important:

Run the Docker exec command in order to apply your specific Docker environment. The command could be run in any point of time after creating and running the Docker container.

It may take up to 10 minutes for the application to start.

The following environment variables can be used when invoking the command:

- **ACCEPT_LICENSE**: (mandatory) Indication that the user has accepted the EULA (End User License Agreement). The value for accepting is the number 1. (For reviewing the license agreement see "reviewing license agreement ")
- **TIME_ZONE**: (optional) use the time zone configured to your monitored device. The time zone should be compatible with the “tz database time zone”. The default time zone is “America/New_York”.
- **DPOD_EXT_HOST_IP**: (optional) Use this variable if your monitored device does not have direct access to your DPOD container (for example, if you are using physical or virtual IDG appliance).
  The value should be the Docker host IP address.
- **DPOD_NTP_1**: (optional) use this value to configure your primary NTP server IP address inside the DPOD container.
- **DPOD_NTP_2**, **DPOD_NTP_3**, **DPOD_NTP_4**: (optional) use this value to configure your secondary NTP servers IP address inside the DPOD container.

Use the following command to display running docker containers:

```
docker ps
```

Access the DPOD container

- Web Console - From your web browser use the container IP address, or more likely your Docker host IP address mapped to the Web

Console port (443 in the example) : https://<IP address>.
user : admin and default password : adminuser

- SSH - Use the container IP address, or more likely your Docker host IP address mapped to the ssh port (9022 in the example) .
  user : root and default password : dpod

Re-run Previously Created DPOD Docker Container

Make sure to replace **DPOD_EXT_HOST_IP** parameter value (currently provided as "**<Host IP Address>**") in the command below with the IP Address of the host machine that runs the Docker containers.

```
docker start dpod  && docker exec -d -u root dpod /bin/su - -c "export
ACCEPT_LICENSE=true; export TIME_ZONE=America/New_York; export
DPOD_EXT_HOST_IP=<Host IP Address>; /app/scripts/app-init.sh"
```

Note : Run the Docker exec command in order to apply your specific Docker environment. The command could be run in any point of time after creating and running the Docker container.

It may take up to 10 minutes for the application to start.

Review License Agreement

For reviewing the license agreement execute the following command. The command can be executed in any stage as long as the container is running.

```
docker exec -t -u root dpod /bin/su - -c "export SHOW_LICENSE=true;
/app/scripts/app-init.sh"
```

Hardware and Software Requirements

Monitored Device (DataPower Gateway) Requirements

- DPOD supports only the supported firmware - 7.2.0.20+, 7.5.0.12+ ,7.5.12+ ,7.5.2.12+, 7.6.0.7+, 7.7.1.1+, 2018.4.1.x
  - However some functionalities are available starting a specific firmware level. For more details please see release notes.
- DPOD supports API Connect v2018.2.5+ (compatibility mode) or v5.0.7.2+
- If any of the the monitored devices attached to DPOD is to be upgraded to firmware versions **7.6.0.0**- **7.6.0.7** you **MUST** upgrade to DPOD 1.0.5.0+ before the firmware upgrade in order to be able to browse transactions from this device.
- If any of the the monitored devices attached to DPOD is to be upgraded to firmware versions **7.6.0.8** OR **7.7.1+** you **MUST** upgrade to DPOD 1.0.8.0+ before the firmware upgrade in order to be able to browse transactions from this device.
- DPOD supports only DataPower with language set to English.

Physical HW or Hypervisor

DPOD can be installed on either a Virtualized Environment (Hypervisors) or Physical server (Intel(C) based CPUs and supporting CentOS 7.x OS). Consult the table below for information to support this decision.

Hypervisor SW

For a production environment suitable for hypervisor (virtual environment), the virtual appliance is supported on the following VMware hypervisors:

- VMWare ESX v5.5 , v6.0, v6.5
- VMWare Player - v12.0 , v12.5
- VMWare Workstation - v12.0 , v12.5, v14
- VMware Fusion v8.0
- PureApp (only on Intel Processors) - no pattern yet available, can be provided only as an imported OVA.
- For Hyper V support - contact your IBM sales representatives.

Resources Requirements

DPOD offers 6 basic load configuration setups.

- One load configuration architecture setup for development that **exists only in the Developer ISO file!** The Developer edition ISO file name is DPOD-**Developer-CentOS-**<version>.iso (Can be download from Fix Central)

- Five load configuration architecture setups that exist for the Standard Edition are available in:
  - Appliance Mode (ISO file) - DPOD_**CentOS**_<version>.iso (Can be download from PPA) - for example: DPOD_**CentOS**_1.0.8.5.iso
  - Non-Appliance Mode (Compressed Executable file) - DPOD_**RedHat**_<version>.cef (Can be download from PPA) - for example: DPOD_**CentOS**_1.0.8.5.cef

The following table lists the typical usage characteristics for each setup edition, and the physical or virtual resources it requires.

Availability in Edition	Load Configuration Architecture Setup	Goal	TPS Limits recommended(4)	Supports Virtual Env	Cores (1)	Memory (3)	Storage (GB)
Developer	Development	Developers only. In rare cases can be used for functional POCs. restricted license	2-3	Yes	2	3 GB	All: 25GB
Standard	Minimal	POCs and Evaluation. Limited history period to reduce memory requirements	5	Yes	4	18 GB	OS: 40 Install: 40 Data(2): 100+
Standard	Low	Environment with low load levels	40	Yes	6	32 GB	OS: 40 Install: 40 Data(2): 100+
Standard	Medium	Environment with Moderate load	80	Yes	8	64GB	OS: 40 Install: 40 Data(2): 300+
Standard	High	Environment with High load	120	Yes, but not recommended	12	128GB	OS: 40 Install: 40 Data(2): 1,000+
Standard	High_20dv	Environment with Medium load	200 Can be increased to 1500 TPS(5)	No. Must be installed on a physical server	16 (Physical)	200GB	OS: 40 Install: 40 Data(2): 2,000

Standard	High_20dv	Environment with High load	1500 TPS[5]	No. Must be installed on a physical server	24 (Physical) [5]	256GB	OS: 40 Install: 40 Data[2+5]: 8,000

Customers who need to handle more than 1500 TPS will be required to install separated multiple nodes.

Customers who expect to handle load over 200 TPS will require to start a sizing process by open ticket to IBM Support - L2.

High Load capacity plan sizing example

A customer wants to attach a pool of appliances to DPOD. This pool generates a peak of circa 10,000 TPS (in average about 35 Syslog records per transaction).

This customer will need to have 7 servers with 2 sockets and 2 Intel based CPUs - each with 12 physical cores of 2.6 Ghz (non turbo) and with hyper-threaded Support . Each server requires 256GB of memory, and storage specification as described below[5].

1 Node = 1500 TPS

7 Nodes = 10,500 TPS.

Each DPOD environment (up to 7 nodes) will support no more than 10,000 TPS.

Customers with higher load still are expected to create separate environments, each can handle up to 10,000 TPS.

Customers who plan to use more than one node or above 1,000 TPS are expected to submit a sizing questionnaire available to IBM technical sales teams.

[1] These could be cores on an 80% utilized ESXi

[2] Local SSD preferred - should be located on a data store separated from the other disks

[3] Best query performance is achieved by using reserved memory configuration

[4] The TPS is the total transaction load across all devices/domains connected to DPOD

IBM DataPower Operations Dashboard may also be installed as a custom distributed edition (not All-in-One) that allows installation on several servers located across separate geographical locations.

This normally requires creating a custom architecture based on a sizing process.

[5] To cater for 1500 TPS, customers are required to have 256GB memory, 24 Physical cores (each is Hyper Threaded thus equivalent to a total of 48), Local storage with RAID0 across 4-8 SSD Disks (SAS 6GBs) - each supporting at least 80K Random Write IOPS 4KiB and write avg latency of less than 35 uSec. Two controllers will be required to be attached to each CPU. Please keep ratio between RAM and Data storage size to be 1GB RAM : 16GB Data Disk (recommended) and no more than 1 GB RAM :32GB DISK (minimal).

Storage Recommendation

- DPOD serves as a database and should therefore be configured to use very fast disks. For this reason, **DPOD installation requires 3 separate DISKS for OS , Installation and Data.**
- Usage of slow disks is not recommended and will impact the amount of time between creation of transaction logs and the availability of the data on DPOD's dashboards.
- For Physical hardware installations that can utilize HW RAID services the following setup is recommend:
  - RAID5 - 40GB - for OS disk
  - RAID5 - 40GB - for App disk
  - RAID0 - Depends on volume - for Data disk.

- For each 1 TB of data 64 GB of RAM is recommended for responsive queries (dashboards and filters). Please keep ratio between RAM and Data storage size to be 1GB RAM : 16GB Data Disk (recommended) and no more than 1 GB RAM :32GB DISK (minimal).

RAID Support
DPOD does not support the CentOS built-in RAID (Software Raid). The only supported RAID is the one handled by a controller

Network Requirements

DPOD requires at least one network interface for accessing DPOD's User Interface and communications with Gateway's Management Interface.

Operating System Requirements - Only applicable to Non Appliance mode

- CentOS 7.5.0/ 7.4.0 / 7.2.0 - x86-64 bit only on supported HW or Hypervisor as stated above
- RHEL 7.2.0 /7.4.0/7.5.0 - x86-64 bit only on supported HW or Hypervisor as stated above Hardware and Software Requirements#Hypervisor SW. (7.3 is not Supported. 7.2 will be out of support in 2019H2)
- Server OS must be a fresh install without any other installed products .
- In Non Appliance mode the OS support is not covered but recommendations will be provided.
- Other 3rd party software products for backups, security and monitoring may be installed. However, due to diversity their impact is unknown.
- During resolution of issues, DPOD support will ask the customer to disable these 3rd party tools, so that issues may be isolated and DPOD verified as their source. Support will not be provided if the 3rd party tools are not disabled.

Client Requirements

DPOD's web user interface requires the following for administration and end users:

- The Web Console requires a minimum screen resolution of 1280 X 720.
- Supported user web browsers are Firefox - latest 2 versions , Internet Explorer 11+ (not Edge) , Chrome - latest 2 versions , Safari - latest 2 versions

Utility Software for Administrators

- An SSH client to connect to the DPOD appliance once installed.
- An FTP Client software to upload/edit files in the appliance when required .

Network Preparation

1. Ensure you have an IP address for the DPOD appliance (including DNS, Default GW, subnet mask and all other network configuration). Throughout this guide, this IP address will be referred to as **<DPOD appliance IP address>**
2. Ensure you have an NTP server available and obtain its IP address.
3. Prepare a list of all your monitored devices with their IP addresses (normally their management IP addresses) and SOMA ports. These are required for the actions in Prepare your Monitored Devices.
4. Ensure ports are open in the firewall during and after the installation in accordance with the requirements set in Firewall Requirements.

Prepare Pre-Installed Operating System

Non Appliance Mode Only
The steps below are only applicable for installation in Non-Appliance mode, and should be performed by your Linux administrator.

- Verify that your operation system is one of the following (x86-64 mode only) as described in system requirements:
    - Red Hat Enterprise Linux Server release 7.2, 7.4, 7.5 or 7.6 (7.3 is not supported)
    - CentOS version 7.2 / 7.4 / 7.6
- Ensure to select the correct architecture type and that all resources listed in system requirements are made available.
- Ensure you have at least one network card installed and configured with full access to network services such as DNS and NTP (the same as your IDGs) - see Network requirements

#	Subject	Action	Checke
	Prepare Admin access	Installation **must** be performed by a root user. You can **NOT** run it with sudo. You can run it after running the command: su -	☑
	Prepare Store service dedicated OS user and group	The Store service requires a dedicated OS user and group to run. User can use the following command : groupadd storeadms && useradd -g storeadms -md /home/storeadm -s /bin/bash storeadm	☑
	Configure OS locale	The supported OS locale is en_US.UTF-8. Use the following procedure to check the supported locale configuration and change it if necessary	☑
	Prepare your installation file and environment	Ensure your /tmp directory has at least 1GB of free space Installation from a different directory is possible. If you opt to run the install from a directory other than /tmp, ensure that this directory: - Has at least 1GB of free space - Is NOT one of these folders: - /app - /logs - /data - /shared - /installs	☑
		Download the CEF file and transfer it to the /tmp directory on the pre-installed OS server.	☑
		Execute the following command from the pre-installed OS server terminal: **chmod 755 ./<File Name>**	☑
	Setup your network (consult your network admin)	Setup DNS - your network admin may need to assist you with this action.	☑
		Setup NTP - it has to be the same used for your IBM DataPower Gateways. - Consult your Linux and network admin about the proper way to configure this service. - Ensure the NTP RPM is installed. Consider executing the following command: - **yum install ntp** - **ntpdate <ntp server hostname>** - **systemctl enable ntpd.service** - **systemctl start ntpd.service**	☑
		Verify that the /etc/hosts file includes an entry with your server name mapped to your external server IP - To find your server name, execute the command: **hostname**	☑

	Verify all required RPMs are installed	Verify the existence of the following RPMs from the official RedHat/CentOS yum repositories: • httpd **version 2.4.6-67 and above** (together with the following dependencies: mailcap, apr, httpd_tools) • mod_ssl • curl • wget • unzip • iptables • iptables-services • bc • fontconfig The installation is usually performed by executing: **yum install httpd mod_ssl curl wget unzip iptables iptables-services bc fontconfig** If this command can not find the package on account of it not being included in the repository, you will need to add the containing repository or manually download the RPMs files and install them. **RedHat Only** - Execute the following command: **subscription-manager repos --enable=rhel-7-server-rh-common-rpms**	☑
		Ensure the httpd service is enabled by executing the command: **systemctl enable httpd.service**	☑
		Ensure the httpd service is started by executing the command: **systemctl start httpd.service**	☑
		Install mod_proxy_html • This RPM is not always accessible from existing repositories. Try first to install it by executing the command: **yum install mod_proxy_html** If you get the error "No package mod_proxy_html available. Error: Nothing to do", you will need to download the RPM yourself, using one of the following methods: • Method 1 - download the RPM • Find your httpd version by executing the command: rpm -qa | grep httpd • The system will print something resembling httpd-**2.4.6-67.el7_2.4**.x86_64. This is the mod_proxy version you need to download • **RedHat Only** - Download the mod_proxy with the correct version from the following url: https://access.redhat.com/downloads/content/mod_proxy_html/2.4.6-45.el7/x86_64/f21541eb/package (change the version part of the url to match the httpd version you found above). Use wget or any other mechanism to download, and ensure to place the RPM inside the /tmp directory of the pre-installed OS server. • Install the RPM by executing the command: rpm -Uvh mod_proxy_html-2.4.6-67.el7_2.4.x86_64.rpm (Note: your version may vary, as described above) • Method 2 - add a repository and install it from the repository using the commands (**RedHat Only**) • **subscription-manager repos --enable=rhel-7-server-optional-rpms** • **yum install mod_proxy_html**	☑
		OPTIONAL - Install kibana **oss** (kibana-oss-6.6.1) This RPM is required only if you would like to manually query the Big Data store. Download the RPM from: https://artifacts.elastic.co/downloads/kibana/kibana-oss-6.6.1-x86_64.rpm Please follow instructions on https://www.elastic.co/guide/en/kibana/6.6/rpm.html#install-rpm Configure kibana (kibana.yml): • server.port: 5601 • server.host: "montier-es-http" • server.basePath: "/op/kibana" • elasticsearch.hosts: "http://montier-es-http:9200" • elasticsearch.shardTimeout: 300000	☑

Prepare disk, mount points / file systems and logical volume

> Tuning requirement - define 3 Disks with LVM and with size and mount points as defined below

✓

For both Production and Non Production installations, the Standard Edition requires 3 disks (LUNs / physical / virtual) to support throughput.

You will need to allocate the following mount points / file systems on the different disks as described in **table 1** below

It is strongly recommended to use logical volume manager (LVM) - particularly for data disks.

This can be done during RHEL installation by choosing ***Installation Destination*** option. You will then need to select all Local Standard drives and choose option ***"I will configure partitioning"*** under the *"**Other Storage Options**"* section.

You should follow table 2 and add all mount points with required definitions using the "+" button.

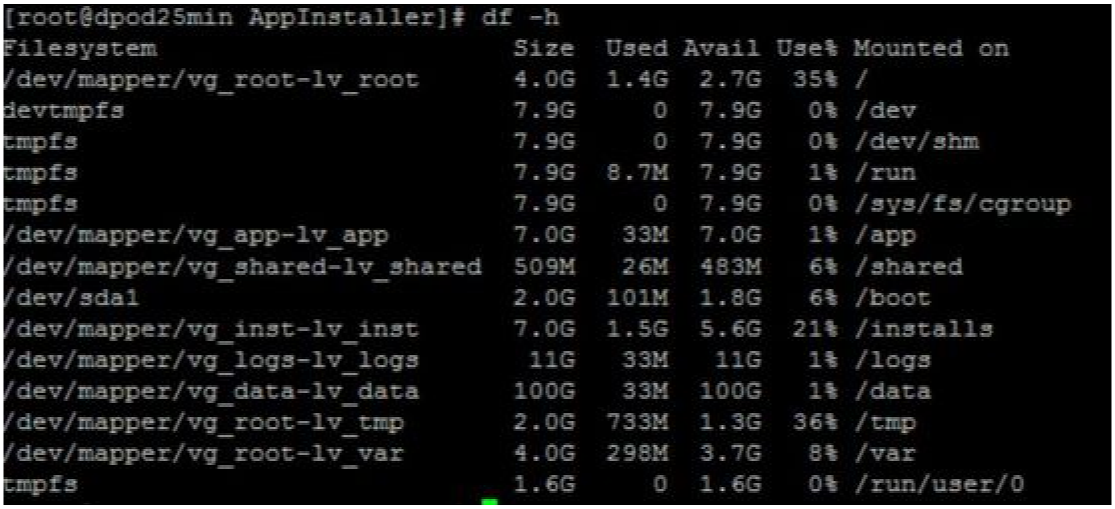
to create a volume group (sys, app, data) open the ***"Volume Group"*** list box and choose ***"create new volume group ..."***

This way you can partition your 3 (logical) drive exactly as stated in table 2.

The minimum file system sizes for the different installation types are described in **table 2** below

After configuring the required mount points you can use the command "df -h" to make sure all free space requirements are met.

Your mount point configuration should resemble the following :



```
[root@dpod25min AppInstaller]# df -h
Filesystem                         Size  Used Avail Use% Mounted on
/dev/mapper/vg_root-lv_root        4.0G  1.4G  2.7G  35% /
devtmpfs                           7.9G     0  7.9G   0% /dev
tmpfs                              7.9G     0  7.9G   0% /dev/shm
tmpfs                              7.9G  8.7M  7.9G   1% /run
tmpfs                              7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/mapper/vg_app-lv_app          7.0G   33M  7.0G   1% /app
/dev/mapper/vg_shared-lv_shared    509M   26M  483M   6% /shared
/dev/sda1                          2.0G  101M  1.8G   6% /boot
/dev/mapper/vg_inst-lv_inst        7.0G  1.5G  5.6G  21% /installs
/dev/mapper/vg_logs-lv_logs         11G   33M   11G   1% /logs
/dev/mapper/vg_data-lv_data        100G   33M  100G   1% /data
/dev/mapper/vg_root-lv_tmp         2.0G  733M  1.3G  36% /tmp
/dev/mapper/vg_root-lv_var         4.0G  298M  3.7G   8% /var
tmpfs                              1.6G     0  1.6G   0% /run/user/0
```

Open your firewall to access to DPOD server

To configure your firewall for open access to the DPOD server for port 443, execute the following commands:

> These commands may not be applicable if your system has no builtin firewall.

firewall-cmd --zone=public --add-port=443/tcp --permanent

firewall-cmd --reload

iptables-save | grep 443

If, for any reason, you need to remove this access (close the port) - execute the following commands:

firewall-cmd --zone=public --remove-port=443/tcp --permanent

firewall-cmd --reload

iptables-save | grep 443

> You should open port access for the DNS Server, your DataPower devices, your SMTP server and others as described in firewall rules.
>
> Please assist your network admin and Linux admin to enable access on these ports.

Table 1 - Prepare your disk and mount points

File system / Mount point	Disk Name
/	sys
/var	sys
/tmp	sys
/boot	sys
swap	sys
/logs	app
/data	data
/shared	app
/app	app
/app/tmp	app
/installs	app

Table 2 - Prepare your file system

Directory / Mount point	**Recommended** **Disk**	**Standard Edition - Minimal/Low/Medium/High** **free space in Mib**	**Device** **Type**	**File** **System**
/	sys	4096	LVM	XFS
swap	sys	8192	swap	XFS
/var	sys	4096	LVM	XFS
/tmp	sys	2048 (recommended 16384)	LVM	XFS
/boot	sys	2048	Standard Partition	XFS
/shared	app	512	LVM	XFS
/app	app	8192	LVM	XFS
/app/tmp	app	4096	LVM	XFS
/installs	app	8192	LVM	XFS
/logs	app	12,288 (can be on other fast disk - preferred locally)	LVM	XFS
/data	data	As described in Hardware and Software Requirements minimum of 100GB	LVM	XFS
/boot/efi	data	For UEFI installations for GPT partition 200	Standard Partition	EFI System Partition

Installation Compatibility Checks

There are two types of checks: Critical and Informational.

The critical checks are mandatory in order to install the system. The informational checks are highly recommended for system optimization.

Please take time to review the results of these checks after installation, and perform all applicable optimizations. The compatibility checks report can be found in /installs/logs/appliance_checks-<date time>.log

Supported programs

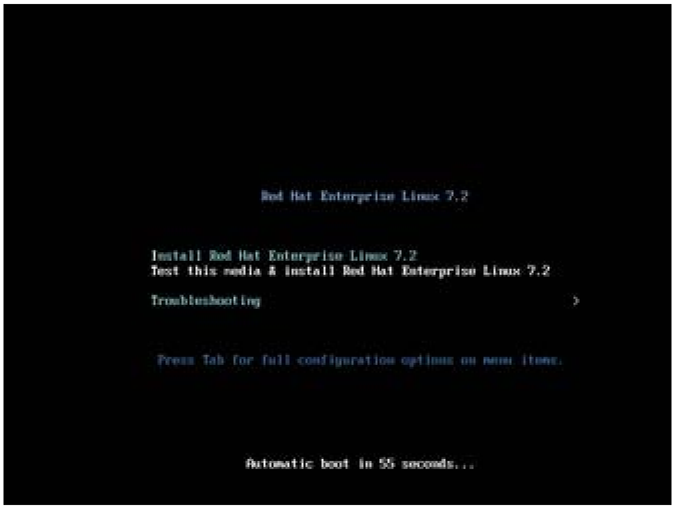
The only supported programs for installation on the DPOD server are infrastructure / system tools like Antivirus agents, Monitor Agents, Backup Agents etc.

Note that these system tools may affect DPOD's functionality and performance.

If you encounter functionality or performance issues, try first to disable these system tools.

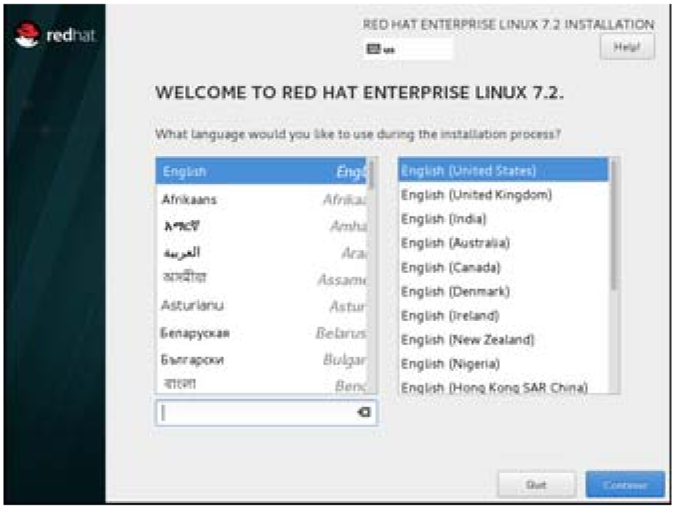
EXAMPLE OF DPOD INSTALLATION ON EXISTING RHEL 7.2 ON VMWARE

1. Download RHEL 7.2 DVD ISO file (not binary boot unless you have access to network installation).
2. Create a VM , assign to ISO file to the VM DVD and start the VM Guest.
3. Press Enter in the first menu



```
Red Hat Enterprise Linux 7.2

Install Red Hat Enterprise Linux 7.2
Test this media & install Red Hat Enterprise Linux 7.2

Troubleshooting                                        >

Press Tab for full configuration options on menu items.

Automatic boot in 55 seconds...
```

4. Choose language

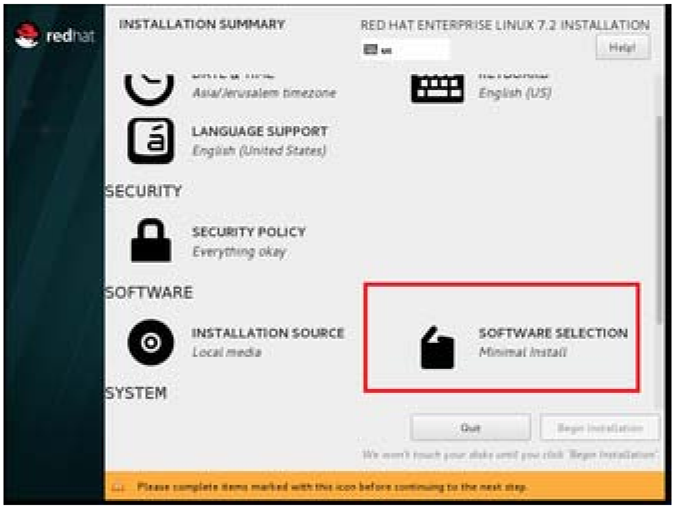


WELCOME TO RED HAT ENTERPRISE LINUX 7.2.

What language would you like to use during the installation process?

English	English	English (United States)
Afrikaans	Afrikaans	English (United Kingdom)
አማርኛ	Amharic	English (India)
العربية	Arabic	English (Australia)
অসমীয়া	Assamese	English (Canada)
Asturianu	Asturian	English (Denmark)
Беларуская	Belarusian	English (Ireland)
Български	Bulgarian	English (New Zealand)
বাংলা	Bengali	English (Nigeria)
		English (Hong Kong SAR China)

5. Choose "Minimal Install" withe no Adds-On in **software selection**



DATE & TIME
Asia/Jerusalem timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SECURITY

SECURITY POLICY
Everything okay

SOFTWARE

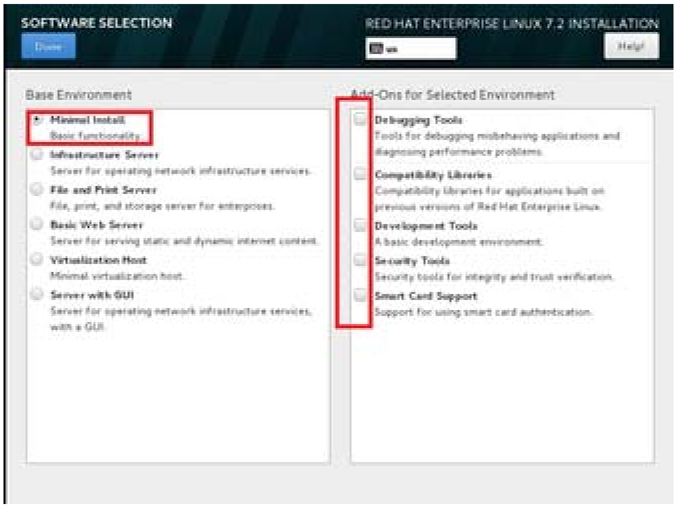
INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.



SOFTWARE SELECTION

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

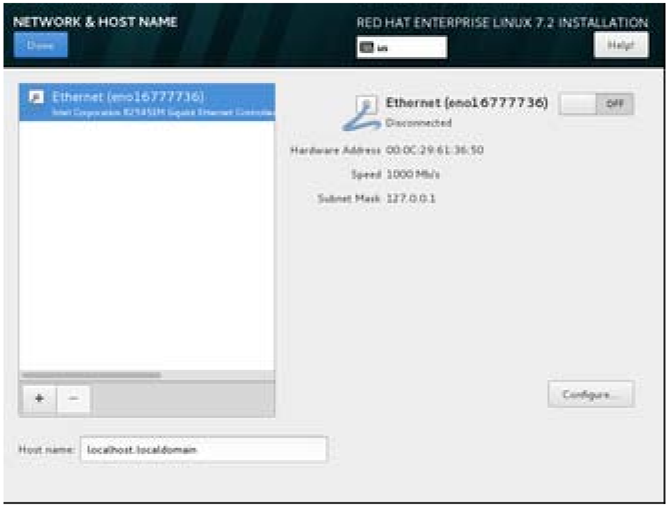
Base Environment

- ● Minimal Install
  Basic functionality.
- ○ Infrastructure Server
  Server for operating network infrastructure services.
- ○ File and Print Server
  File, print, and storage server for enterprises.
- ○ Basic Web Server
  Server for serving static and dynamic internet content.
- ○ Virtualization Host
  Minimal virtualization host.
- ○ Server with GUI
  Server for operating network infrastructure services, with a GUI.

Add-Ons for Selected Environment

- □ Debugging Tools
  Tools for debugging misbehaving applications and diagnosing performance problems.
- □ Compatibility Libraries
  Compatibility libraries for applications built on previous versions of Red Hat Enterprise Linux.
- □ Development Tools
  A basic development environment.
- □ Security Tools
  Security tools for integrity and trust verification.
- □ Smart Card Support
  Support for using smart card authentication.

6. Disable network by press on the OFF button. If Static IP configuration required press configure



NETWORK & HOST NAME

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

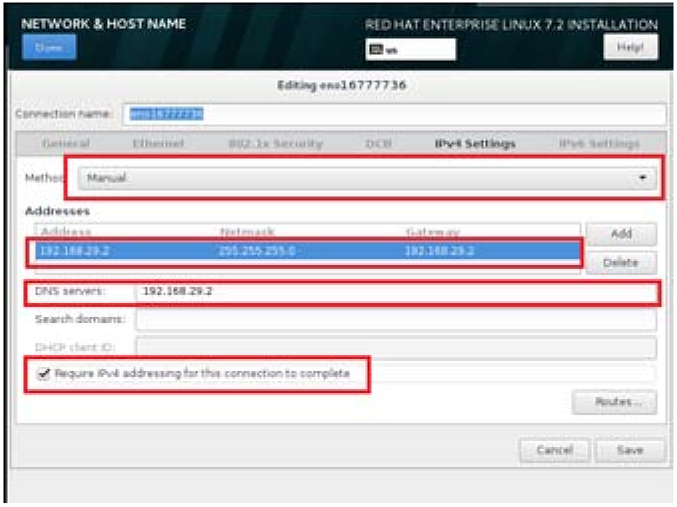
Ethernet (eno16777736)
Intel Corporation 82545EM Gigabit Ethernet Controller

Ethernet (eno16777736) OFF
Disconnected

Hardware Address 00:0C:29:61:36:50
Speed 1000 Mb/s
Subnet Mask 127.0.0.1

Host name: localhost.localdomain

   a. Press "Configure" button
   b. in "IPv6 Settings" choose Method "Ignore"
   c. in "IPv4 Settings" set all 4 fields as marked in Red



NETWORK & HOST NAME

RED HAT ENTERPRISE LINUX 7.2 INSTALLATION

Editing eno16777736

Connection name: eno16777736

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.29.2	255.255.255.0	192.168.29.2

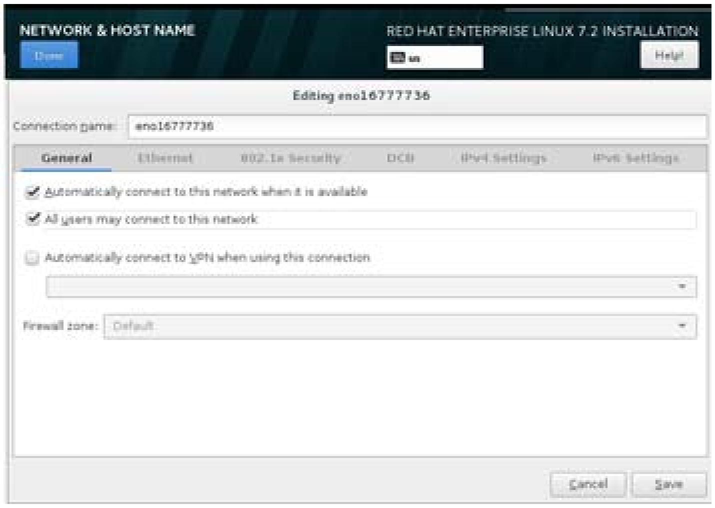
DNS servers: 192.168.29.2

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

   d. set "General" as follow



Editing eno16777736

Connection name: eno16777736

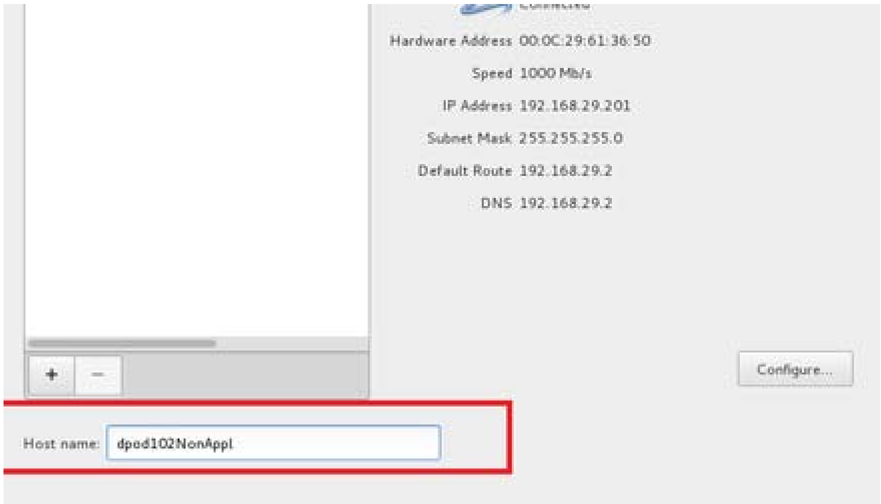
☑ Automatically connect to this network when it is available

☑ All users may connect to this network

☐ Automatically connect to VPN when using this connection

Firewall zone: Default

e. set Host Name



Hardware Address 00:0C:29:61:36:50

Speed 1000 Mb/s

IP Address 192.168.29.201

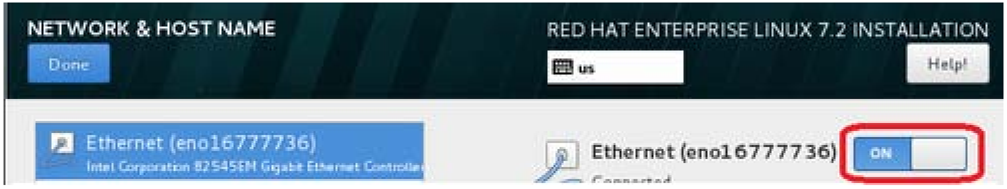
Subnet Mask 255.255.255.0

Default Route 192.168.29.2

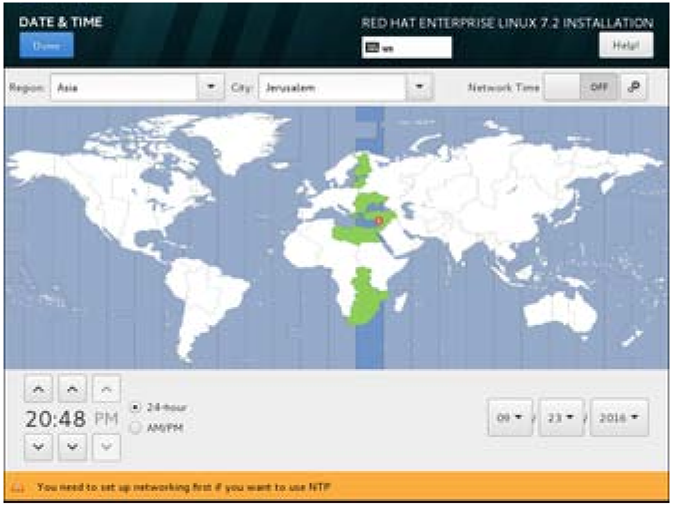
DNS 192.168.29.2

Host name: dpod102NonAppl

f. Enable network by press on the ON button.


NETWORK & HOST NAME
Done
RED HAT ENTERPRISE LINUX 7.2 INSTALLATION
us
Help!
Ethernet (eno16777736)
Intel Corporation 82545EM Gigabit Ethernet Controller
Ethernet (eno16777736)
ON
Connected

7. Change Time Zone and enable NTP



Region: Asia

City: Jerusalem

20:48 PM

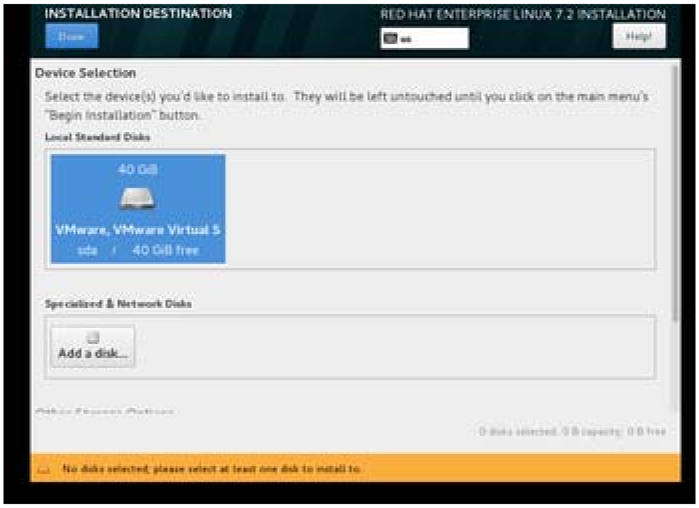
● 24-hour

○ AM/PM

09 / 23 / 2016

You need to set up networking first if you want to use NTP

8. Chose Disk for Installation Destination



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

40 GiB
VMware, VMware Virtual S
sda / 40 GiB free

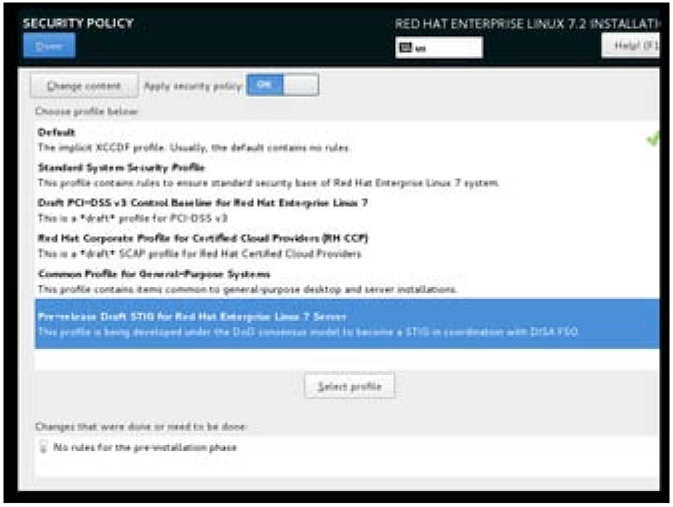
Specialized & Network Disks

Other Storage Options

0 disks selected; 0 B capacity; 0 B free

No disks selected; please select at least one disk to install to.

9. Set security profile



Apply security policy: ON

Choose profile below:

Default ✓
The implicit XCCDF profile. Usually, the default contains no rules.

Standard System Security Profile
This profile contains rules to ensure standard security base of Red Hat Enterprise Linux 7 system.

Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
This is a *draft* profile for PCI-DSS v3

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
This is a *draft* SCAP profile for Red Hat Certified Cloud Providers

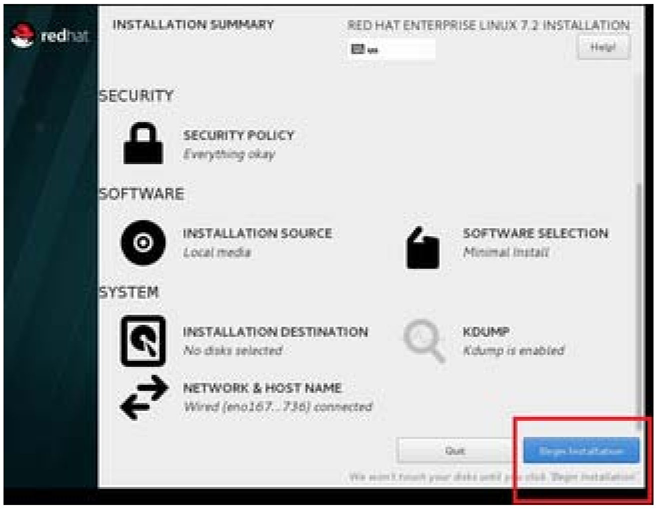
Common Profile for General-Purpose Systems
This profile contains items common to general-purpose desktop and server installations.

Pre-release Draft STIG for Red Hat Enterprise Linux 7 Server
This profile is being developed under the DoD consensus model to become a STIG in coordination with DISA FSO.

Changes that were done or need to be done:

No rules for the pre-installation phase

10. Start Installation by press "Begin Installation" Button



SECURITY

SECURITY POLICY
Everything okay

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

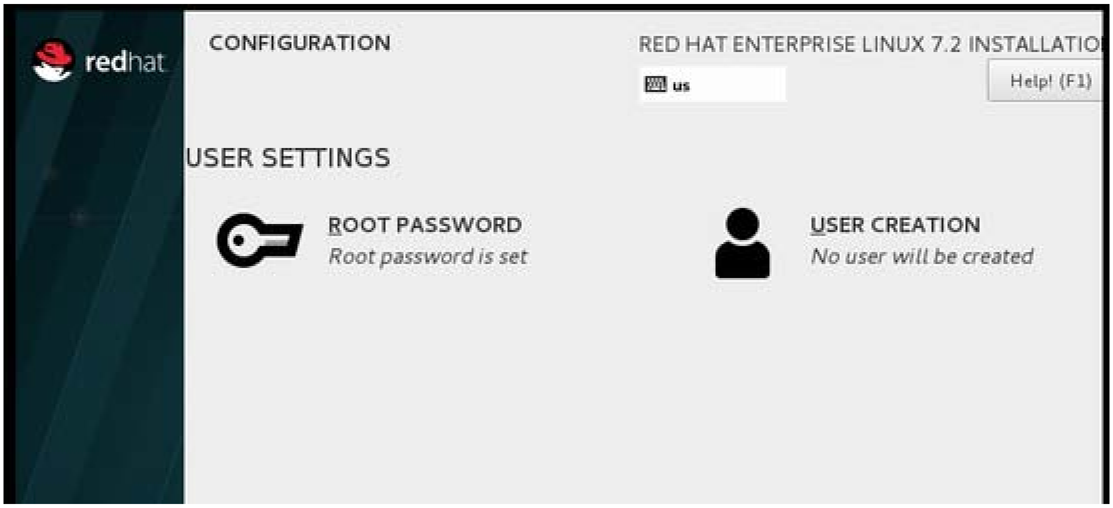
INSTALLATION DESTINATION
No disks selected

KDUMP
Kdump is enabled

NETWORK & HOST NAME
Wired (eno167...736) connected

We won't touch your disks until you click 'Begin Installation'.

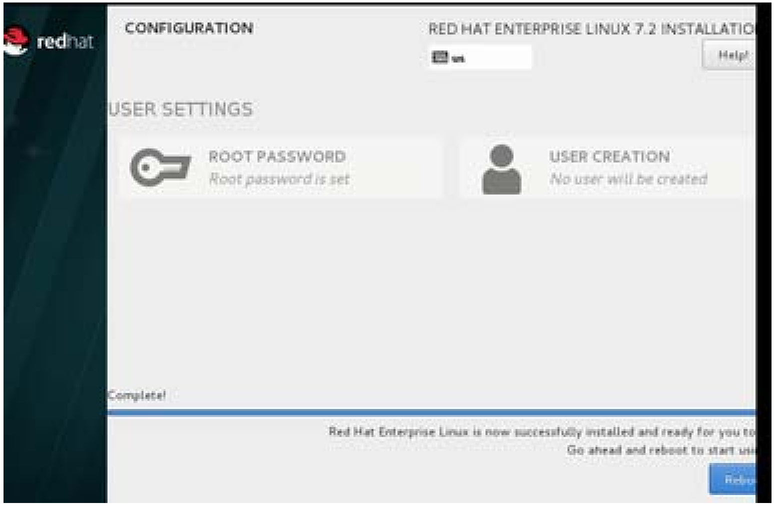
11. Set password for root user



ROOT PASSWORD
Root password is set

USER CREATION
No user will be created

12. Wait for installation to finish and press the reboot button



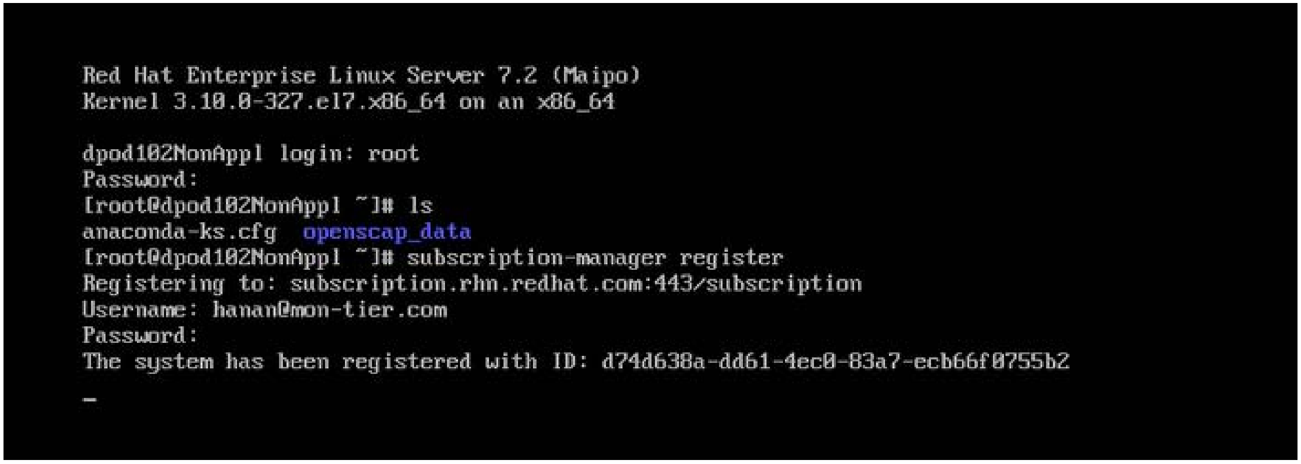
ROOT PASSWORD
Root password is set

USER CREATION
No user will be created

Complete!

Red Hat Enterprise Linux is now successfully installed and ready for you to
Go ahead and reboot to start usi

13. register system **RedHat Only**
    subscription-manager register
    Note: you will need to provide user and password



```
Red Hat Enterprise Linux Server 7.2 (Maipo)
Kernel 3.10.0-327.el7.x86_64 on an x86_64

dpod102NonAppl login: root
Password:
[root@dpod102NonAppl ~]# ls
anaconda-ks.cfg  openscap_data
[root@dpod102NonAppl ~]# subscription-manager register
Registering to: subscription.rhn.redhat.com:443/subscription
Username: hanan@mon-tier.com
Password:
The system has been registered with ID: d74d638a-dd61-4ec0-83a7-ecb66f0755b2
_
```

14. Enable subscription **RedHat Only**

```
subscription-manager attach
```

15. Updates **RedHat Only**

    ```
    install drivers
    ```

16. Install packages: **RedHat Only**

    ```
    subscription-manager repos --enable=rhel-7-server-rh-common-rpms
    ```

    ```
    yum install rhevm-guest-agent-common
    ```

    systemctl start ovirt-guest-agent.service

    ```
    systemctl enable ovirt-guest-agent.service
    ```

Prepare your Monitored Devices

The following steps are required in order to integrate DPOD into your monitored device(s) environment.

1. Prepare Authentication Information

Ensure you have obtained an admin privileged login for each DataPower Gateway. You will use this login to configure the DataPower Gateway for DPOD.

> It is highly recommended you create a dedicated user for DPOD.

2. Prepare Network Time Protocol (NTP)

Ensure each of your monitored devices is configured to use NTP.

DPOD will be configured to use the same NTP Servers as your monitored device(s).

DPOD might produce inconsistent view of the system if its monitored devices do not use the same time source, as the reported time is based on the monitored device time.

3. Perform Required Configuration On Monitored Device(s)

The following steps needs to be performed on each of your monitored devices

1. Set IBM DataPower Gateway System Identifier (also called Appliance Name in firmware 7 and above). This is defined on **[Administration->Device->System Settings->System Identifier / Appliance Name]**:
   important : avoid using spaces in Appliance Names.
2. Configure the services in the XML Management interface **[Network->Management->XML Management Interface]** as follows:
   a. Enable SOAP Configuration Management
   b. Enable AMP Endpoint
   c. Enable SLM Endpoint
   d. Enable WS-Management Endpoint
   e. Firmware 6.X only - Disable (uncheck) SOAP Management URI
   f. Firmware 6.X only - Disable (uncheck) SOAP Configuration Management (v2004)
3. Make sure the XML Management Interface is enabled

4. Backup Your Monitored Device(s)

Before you Add Monitored Devices to DPOD, it is imperative that you take a backup of your entire system.
During the installation process DPOD will:

- ***Create Log Targets automatically once you will initiate that step.***
- Enable system statistics
- Create network aliases for DPOD
- Perform other optional steps (e.g. Certificate Monitoring)

As all these actions potentially alter system configuration, a backup is paramount in case a restore is required later on.

5. Changes to a Gateway that DPOD performs

> Please review this list before using the product.

Please review the changes that DPOD is about to perform to your Gateway and make sure they are acceptable.

You should be aware that not all the changes can be undone automatically and some may require manual intervention to revert.

Please refer to the uninstall procedure before you start

GATEWAY CHANGES PERFORMED BY DPOD

I order for DPOD to be able to gather the information it requires, it enables various features and creates several objects in DataPower.

The table below details the objects and the methods you can use to undo these changes.

Object in Gateway	Action	Explanation	Can it be undone automatically ?
SOMA Configuration (Device Level)	Update	Upon a user request from the Web Console (when adding a Monitored Device) the SOMA Configuration is aligned with the required manual step detailed in the Prepare your Monitored Devices chapter. This request is explicitly accepted by the admin on the UI. If the SOMA configuration is not fully aligned, then DPOD will set it correctly and make the following changes to the XML Management Interface [Network Management XML Management Interface] 1. Enable SOAP Configuration Management 2. Enable AMP Endpoint 3. Enable SLM Endpoint 4. Enable WS-Management Endpoint 5. Firmware 6.X only - Disable (uncheck) SOAP Management URI Firmware 6.X only - Disable (uncheck) SOAP Configuration Management (v2004)	No. To undo these changes, leave this checkbox unchecked when you install DPOD. If a backup is performed as requested in the installation procedure, then this data can be extracted from the backup by restoring it to a temporary Gateway instance and viewing the exact configuration. The specific scripts will then set appropriate values identified in the action above.
Device Statistics	Update	Upon a user request from the Web Console, DPOD enables the device statistics if they were not enabled before. This request is explicitly accepted by the admin on the UI.	No. To undo this change, leave this checkbox unchecked when you install DPOD. If a backup is performed as requested in the installation procedure, then this data can be extracted from the backup by restoring it to a temporary Gateway instance and viewing the exact configuration. The specific scripts will then set appropriate values identified in the action above.
Host Alias (Device Level)	Add	Upon a user request from the Web Console, two host aliases will be created - "MSC-(env name)" (or montier-syslog in older DPOD versions) and MonTier_LogTarget_Source. The alias montier-wsm will be created on the first creation of a WSM subscription.	Yes, it can be removed with a script.
Log Target (Device Level)	Add	Upon a user request from the Web Console (by clicking a button), One log target called DPOD-MSC-<env name>-system will be added in default domain (if the setup was done before DPOD v1.0.5 the log target name will be MonTier-system-log).	Yes, it can be removed with a script. Or, when deleting a monitored device via ManageDevices>Monitored DevicesDelete Device, check the box "Delete Syslog logs targets from device" in the confirmation window.
Log Target (Domain Level)	Add	Upon a user request from the Web Console (by clicking a button), Two log target are created for each existing domain at the time of running the action from DPOD's web console. The log target names are DPOD-MSC-<env name>-1 and DPOD-MSC-<env name>-2 (or montier-syslog-1 and montier-syslog-2 if the setup was done before DPOD v1.0.5) For API Connect domains, there may be a third log target called DPOD-MSC-<env-name>-3 Domains added subsequently may not have these 2 DPOD log targets (unless they were setup via "Auto setup domains")	Yes, it can be removed with a script. Or, when deleting a monitored device via ManageDevices>Monitored DevicesDelete Device, check the box "Delete Syslog logs targets from device" in the confirmation window.
Log Category (Device Level)	Add	Upon a user request from the Web Console (by clicking the "Setup Syslog" on a device) a new log category, msc-mon, is added.	Yes, it can be removed with a script.

Certificate Monitor	Update	Upon a user request from the Web Console, DPOD sets this object in the admin state to 'enabled' and changes the interval and Reminder time.	No. If a backup is performed as requested in the installation procedure, then this data can be extracted from the backup by restoring it to a temporary Gateway instance and viewing the exact configuration. The specific scripts will then set appropriate values identified in the action above.
Extended Transaction Device Level	Add	Upon a user request from the Web Console, a user Log Category (montier-mon) is added to mark DPOD special logs.	Yes, it can be removed with a script.
	Add	Upon a user request from the Web Console, this action copies the following files to the Gateway store directory - store://Montier-LOG.xsl, and store:///Montier-IDcheckSet.xsl:	Yes, it can be removed with a script.
Extended Transaction Service & Domain Level	Update	Create Checkpoint - Before adding a stylesheet to easy recover, DPOD creates a checkpoint and performs a backup.	No, the checkpoint cannot be undone automatically.
	Update	Since an Extended transaction is intrusive by nature (as documented), DPOD adds Transform Action rule to the end of each rule for each Processing Policy for each WSP, MPG that exists in this domain. Since this is an Intrusive action, the appropriate alert will appear – see Appendix A for a reference to the documentation.	Partially. If no new Actions were added after the Action was added by DPOD then a customer script can remove it but Support can not provide such functionality.
WS-M Agent definition Device Level	Update	For each domain in the device, DPOD modifies the Web Service Management Agent [ObjectsWeb Service Management Agent]: 1. Change attribute "Maximum Memory Usage" to 102400 2. Change attribute "Capture Mode" to All DPOD doesn’t change the admin state of the objects, therefore DPOD changes the gateway configuration only if this feature is used.	To undo these changes, the state of this checkbox needs be kept before you install DPOD. If a backup is performed as requested in the installation procedure, then this data can be extracted from the backup by restoring it to a temporary Gateway instance and viewing the exact configuration. The specific scripts will then set appropriate values identified in the action above.
WS-M Agent definition Domain Level		For a selected domain in the device, DPOD modifies the Web Service Management Agent [ObjectsWeb Service Management Agent]: 1. Change attribute "Maximum Memory Usage" to 102400 2. Change attribute "Capture Mode" to All DPOD doesn’t change the admin state of the objects, therefore DPOD changes the gateway configuration only if this feature is used.	To undo these changes, the state of this checkbox needs be kept before you install DPOD. If a backup is performed as requested in the installation procedure, then this data can be extracted from the backup by restoring it to a temporary Gateway instance and viewing the exact configuration. The specific scripts will then set appropriate values identified in the action above.
WS-M subscription	Create	This is a temporary object that is used for a predefined amount of time (usually for a few minutes) and when expired it is deleted by Gateway automatically	Not Relevant

This documentation ignores irrelevant changes such as entry to log files.

Installation

Installing IBM DataPower Operations Dashboard

Having completed the Planning and preparations, your system should be ready for the actual installation of IBM DataPower Operations Dashboard.

A typical installation takes circa 30 minutes to complete all three steps below.

> The Appliance installation is configuring system settings (kernel parameters) based on the amount of system allocated memory, these settings are important for the DPOD performance.
>
> It is highly important that on the Appliance OS installation phase the system will have all necessary resources allocated, especially the memory allocation.
>
> If You are installing Non-Appliance installation, a report listing system tests and gaps will be generated, please review the “kernel parameters” section and adjust you system to the recommended values, especially the performance related settings.
>
> For the list of DPOD system settings see OS Kernel settings

In some installation scansion customer will install DPOD not for the first time and would like to migrate data into the new instillation. Please review the Data Migration Procedure.

- Appliance Installation
- Non-Appliance Installation
- Installation Verification
- Data Migration Procedure

Appliance Installation

DPOD acts like a virtual appliance but comes packaged as an ISO file, in order to support installation on both physical and virtual installation scenarios.

When Installing DPOD from an ISO file, The first step is to install the Appliance. This means installation and configuration of the OS that is pre-loaded on the ISO (CentOS).

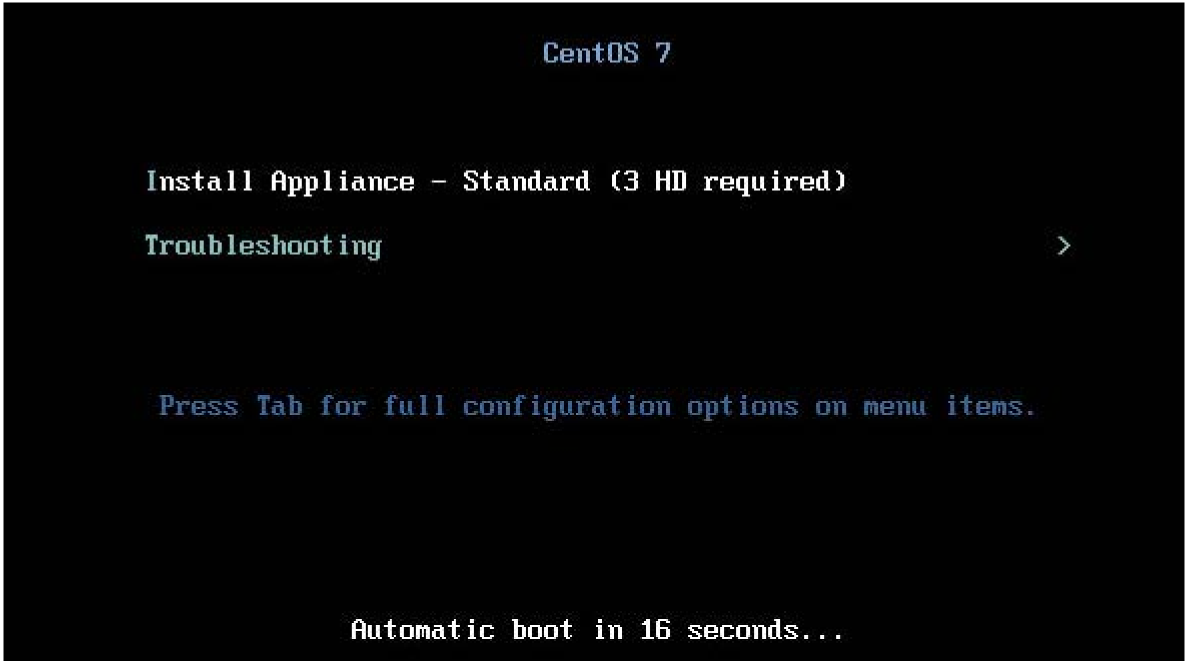
Completing the steps below will create a DPOD-ready appliance to install DPOD's software on.

> You MUST NOT add or install any packages / RPMs at DPOD's installation time (or after installation completes) unless instructed by support.
>
> You MUST NOT update the CentOS version or any other component within DPOD using external repositories (for example, do not use yum update).
>
> The only supported way to upgrade the platform and/or components is by applying a product Fix Pack.

OS Installation

1. Set DPOD ISO file on your virtual/physical server's DVD.
2. Power on the virtual/physical server.

On the OS launch screen, choose “Install Appliance” to start the automatic OS installation for Standard Edition.



CentOS 7

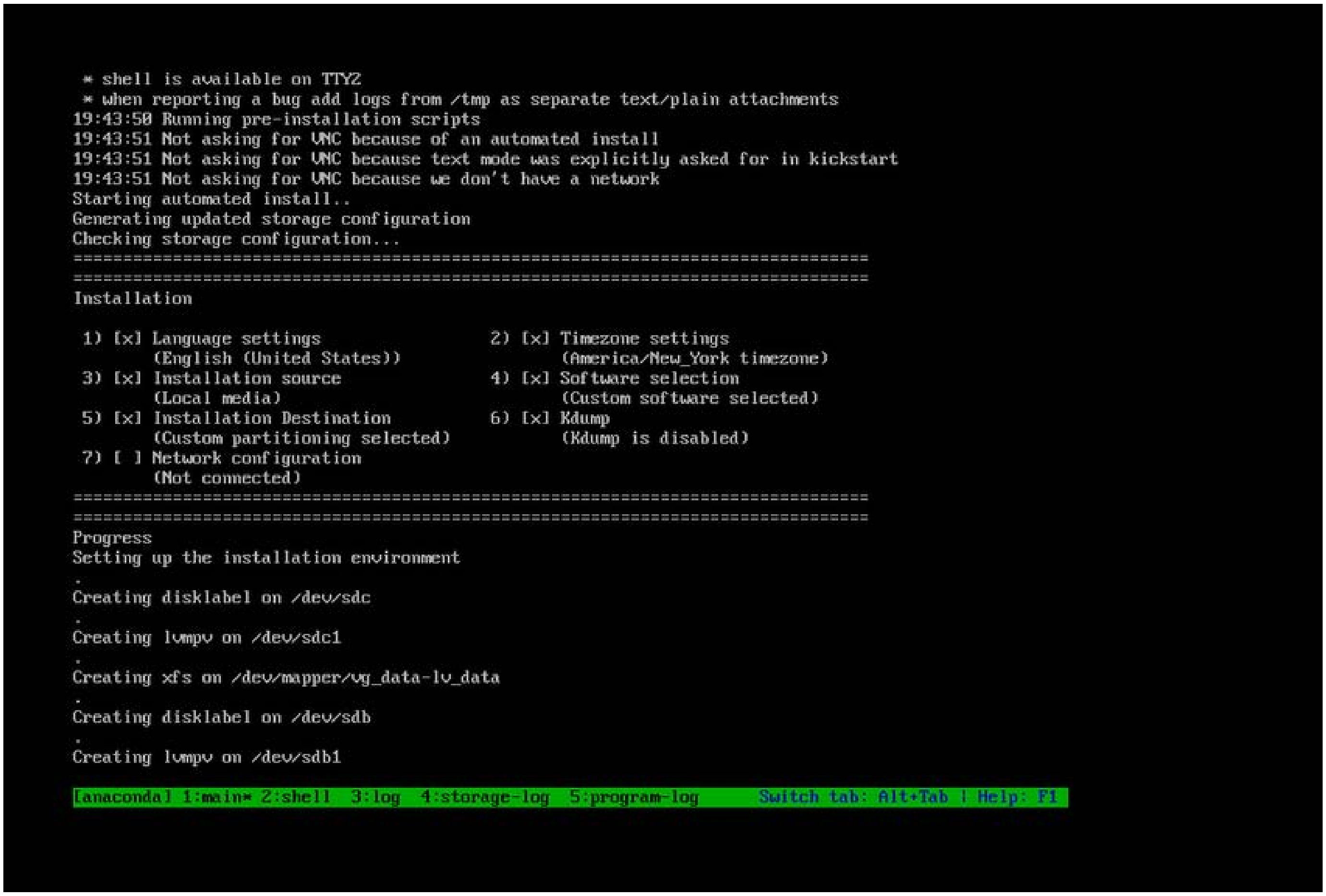
Install Appliance - Standard (3 HD required)

Troubleshooting >

Press Tab for full configuration options on menu items.

Automatic boot in 16 seconds...

The required packages will now be installed. Wait for the installation to complete before proceeding (this should take a few minutes).



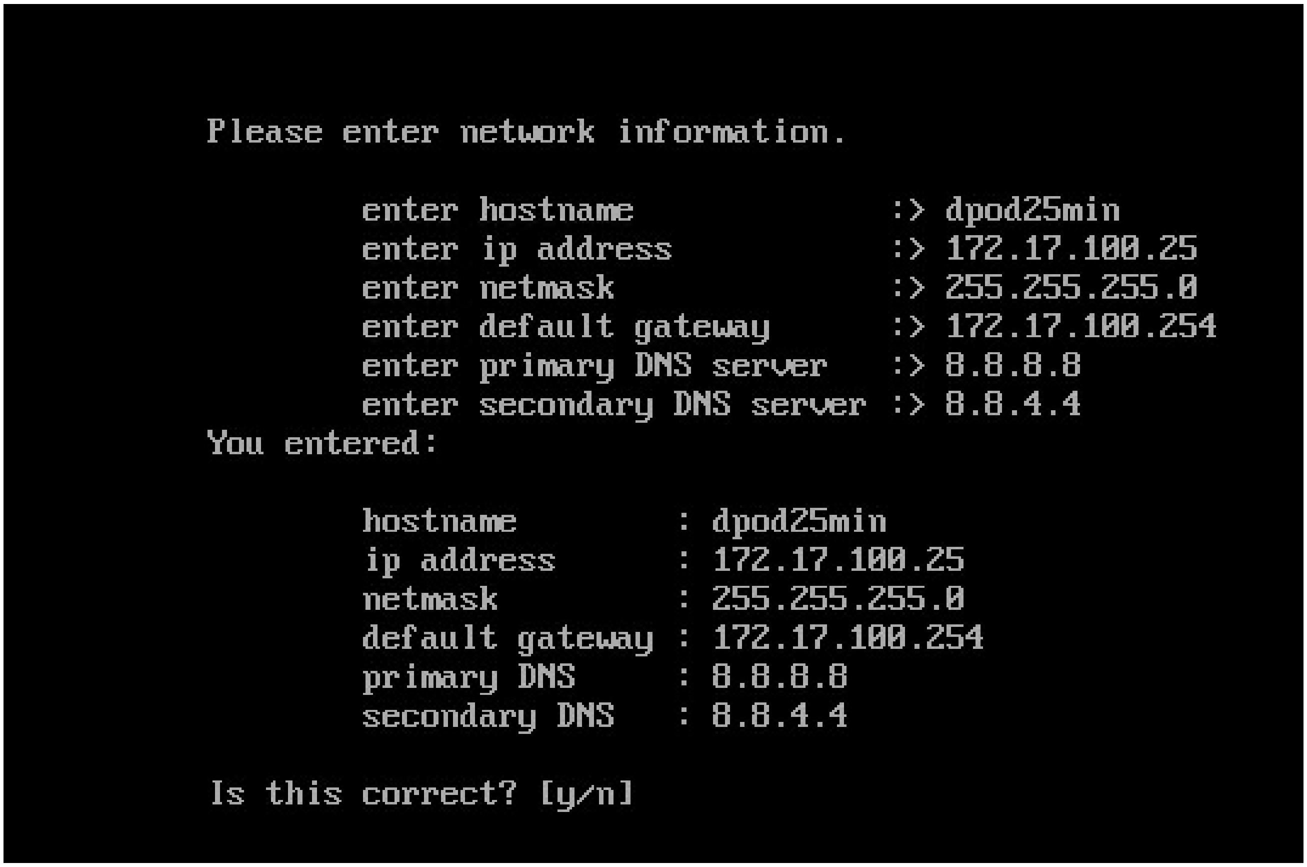
```
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
19:43:50 Running pre-installation scripts
19:43:51 Not asking for VNC because of an automated install
19:43:51 Not asking for VNC because text mode was explicitly asked for in kickstart
19:43:51 Not asking for VNC because we don't have a network
Starting automated install..
Generating updated storage configuration
Checking storage configuration...
================================================================================
================================================================================
Installation

 1) [x] Language settings                 2) [x] Timezone settings
        (English (United States))                (America/New_York timezone)
 3) [x] Installation source               4) [x] Software selection
        (Local media)                            (Custom software selected)
 5) [x] Installation Destination          6) [x] Kdump
        (Custom partitioning selected)           (Kdump is disabled)
 7) [ ] Network configuration
        (Not connected)
================================================================================
================================================================================
Progress
Setting up the installation environment
.
Creating disklabel on /dev/sdc
.
Creating lvmpv on /dev/sdc1
.
Creating xfs on /dev/mapper/vg_data-lv_data
.
Creating disklabel on /dev/sdb
.
Creating lvmpv on /dev/sdb1

[anaconda] 1:main* 2:shell  3:log  4:storage-log  5:program-log      Switch tab: Alt+Tab | Help: F1
```

Developer Edition should have different launch screen stating this is a Developer Edition. The rest of the steps are the same

Network Configuration

When the OS installation completes, you will be presented with the Network Configuration screen, used to provide DPOD with the network information it requires.

1. Enter DPOD's host name, e.g. dpod25min (you may add the host name to your organization's DNS).
2. Enter the IPv4 address, e.g. 192.168.65.170
3. Enter the network netmask, e.g. 255.255.255.0
4. Enter the default gateway: e.g. 192.168.65.2
5. Enter primary and secondary DNS server IP addresses (not mandatory)



```
Please enter network information.

        enter hostname              :> dpod25min
        enter ip address            :> 172.17.100.25
        enter netmask               :> 255.255.255.0
        enter default gateway       :> 172.17.100.254
        enter primary DNS server    :> 8.8.8.8
        enter secondary DNS server :> 8.8.4.4
You entered:

        hostname        : dpod25min
        ip address      : 172.17.100.25
        netmask         : 255.255.255.0
        default gateway : 172.17.100.254
        primary DNS     : 8.8.8.8
        secondary DNS   : 8.8.4.4

Is this correct? [y/n]
```

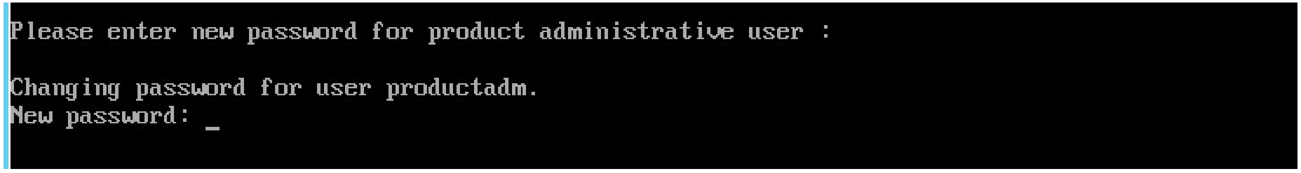
When the network data entry process is complete, DPOD echoes it back on the screen for verification and displays an 'Is this correct [y/n]' prompt.

Enter “y” to confirm network details as entered or “n” to re-enter the information.

Setting Admin Passwords

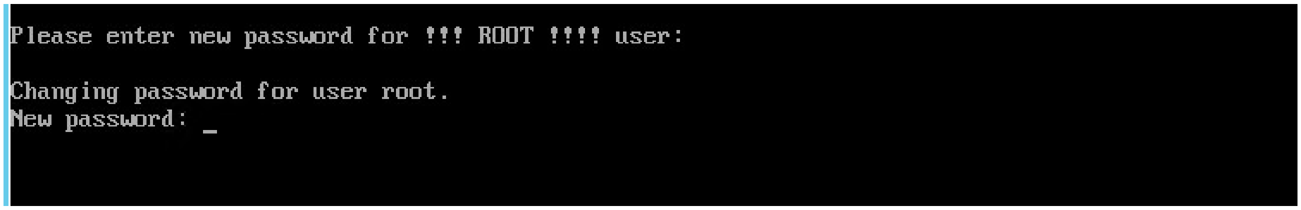
The last screen lets you set passwords for the admin users.

1. Change DPOD's OS administrative user (productadm) password:



```
Please enter new password for product administrative user :

Changing password for user productadm.
New password: _
```

2. Change root user password .

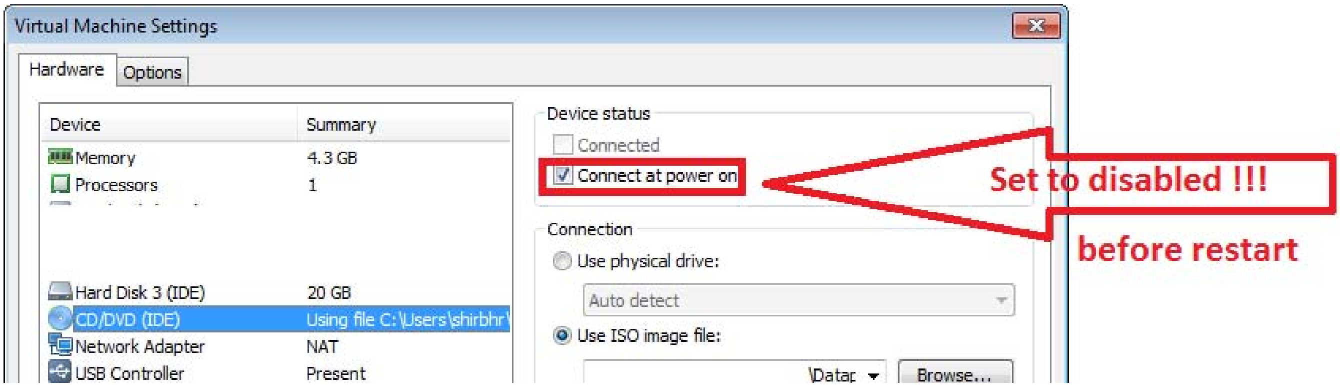


```
Please enter new password for !!! ROOT !!!! user:

Changing password for user root.
New password: _
```

Installation Finalization

When you've completed all the steps above, before you press **ENTER or Return** you should disable/ Eject your DVD of DPOD.

In VMWare you can do it by edit the VM Host setting and disable the following



Virtual Machine Settings

Device	Summary
Memory	4.3 GB
Processors	1
Hard Disk 3 (IDE)	20 GB
CD/DVD (IDE)	Using file C:\Users\shirbhr\
Network Adapter	NAT
USB Controller	Present

Device status

□ Connected

☑ Connect at power on

Connection

○ Use physical drive:

Auto detect

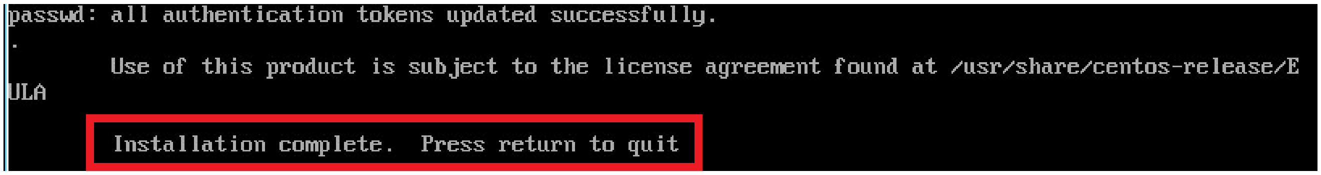
● Use ISO image file:

\Datap

Set to disabled !!!

before restart

Please press **ENTER or Return** and the server will restart automatically.



```
passwd: all authentication tokens updated successfully.
.
        Use of this product is subject to the license agreement found at /usr/share/centos-release/E
ULA

         Installation complete.  Press return to quit
```

After the server was restarted - don't forget to remove the DPOD installation disc from the DVD drive.

Next: Run the Software Deployment

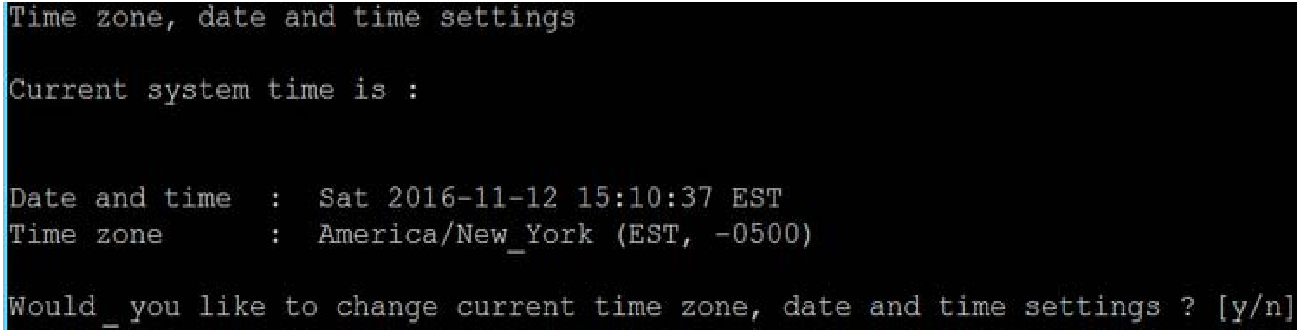
SOFTWARE DEPLOYMENT

The steps described in this page will walk you through the process of deploying DPOD's software on the appliance created in the Appliance Installation phase.

1. Log in to DPOD's VM Console with the user "root" (Do not use an SSH terminal here. For security reasons, SSH sessions are limited to 300 seconds and your session might time out during installation).
2. run "df -h" and make sure the three required disks were mounted and are in the correct order (OS, Install and Data disks, as explained on Hardware and Software Requirements)
3. Run the installApp command to start the product installation:

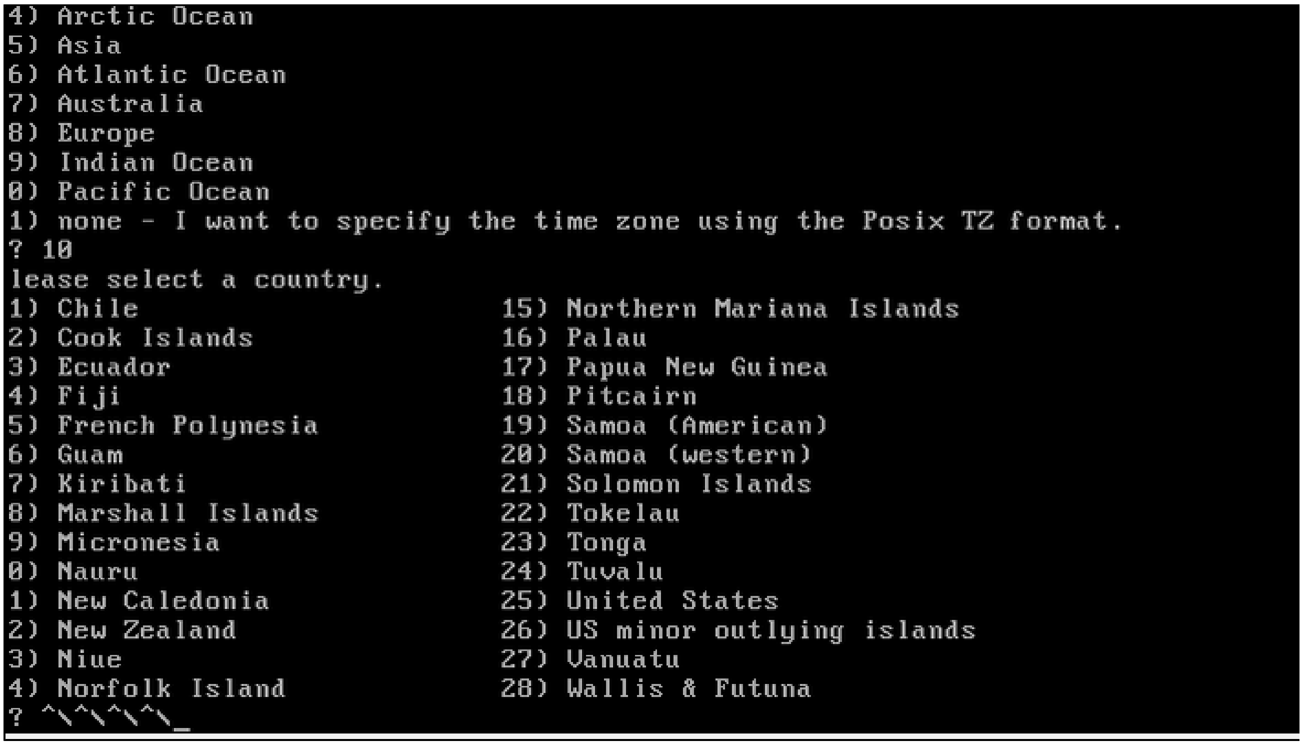
```
installApp
```

4. Adjust Date, Time and TimeZone if required



```
Time zone, date and time settings

Current system time is :


Date and time   :  Sat 2016-11-12 15:10:37 EST
Time zone       :  America/New_York (EST, -0500)

Would_ you like to change current time zone, date and time settings ? [y/n]
```

If you choose to change current time zone configuration you will be prompted for time zone selection :



```
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
0) Pacific Ocean
1) none - I want to specify the time zone using the Posix TZ format.
? 10
lease select a country.
1) Chile                      15) Northern Mariana Islands
2) Cook Islands               16) Palau
3) Ecuador                    17) Papua New Guinea
4) Fiji                       18) Pitcairn
5) French Polynesia           19) Samoa (American)
6) Guam                       20) Samoa (western)
7) Kiribati                   21) Solomon Islands
8) Marshall Islands           22) Tokelau
9) Micronesia                 23) Tonga
0) Nauru                      24) Tuvalu
1) New Caledonia              25) United States
2) New Zealand                26) US minor outlying islands
3) Niue                       27) Vanuatu
4) Norfolk Island             28) Wallis & Futuna
? ^\^\^\^\_
```

a. Select your country's region, for example: Pacific Ocean (number 10)
b. Select your country, for example: Singapore (number 40)

DPOD will suggest a time zone based on your country selection, and display an 'Is the above information OK?' prompt. You may confirm the time zone configured by choosing 1 for “yes” or 2 for “no”.

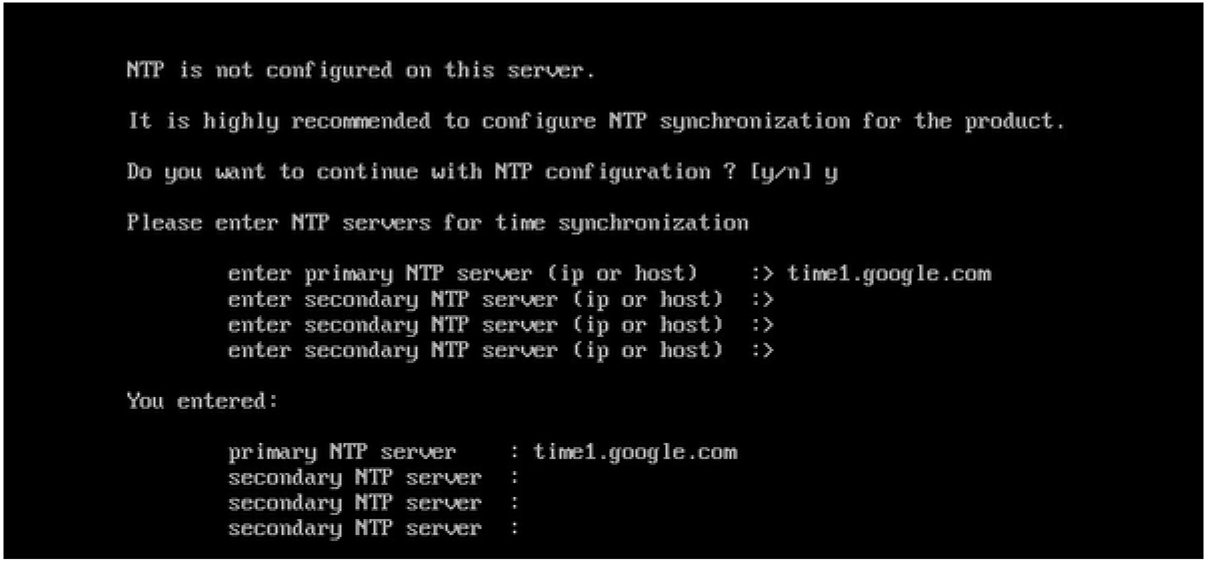
If you reject the proposed time zone,you will nee to select the right one for you.

- Enter the current date and time in the format of YYYY-MM-DD hh:mm:ss, for example: 2017-07-10 14:00:00

5. On the next screen you configure the NTP (Network Time Protocol) servers DPOD is going to use. Keeping the internal clocks of DPOD and the monitored appliances in sync is important - as DPOD reports the time as logged by the devices themselves.

   Enter your NTP servers information
   a. DPOD displays a 'Do you want to continue with NTP configuration' prompt. Enter "y" to continue with NTP configuration or "n" to skip.
   b. Enter at least one NTP server (more than 2 is recommended)

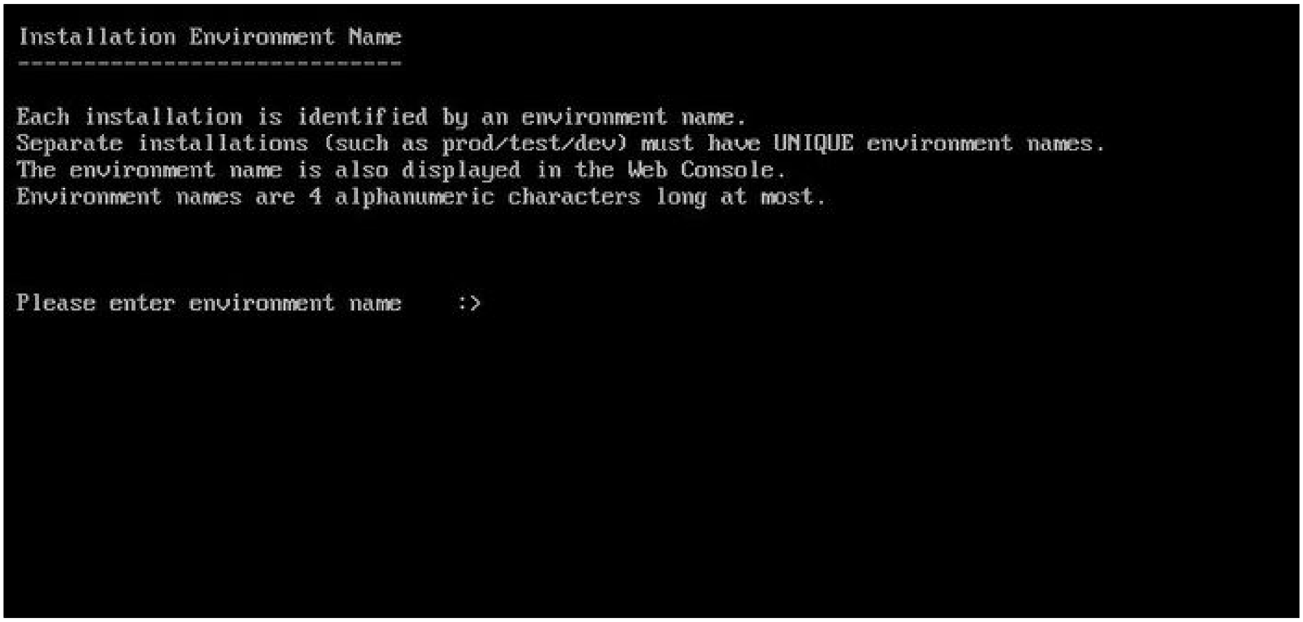
   After you finish entering the NTP data, DPOD echoes it back on the screen for verification and displays an 'Is this correct [y/n]' prompt. Enter “y” to confirm NTP details as entered or “n” to re-enter the information.



```
NTP is not configured on this server.

It is highly recommended to configure NTP synchronization for the product.

Do you want to continue with NTP configuration ? [y/n] y

Please enter NTP servers for time synchronization

        enter primary NTP server (ip or host)    :> time1.google.com
        enter secondary NTP server (ip or host)  :>
        enter secondary NTP server (ip or host)  :>
        enter secondary NTP server (ip or host)  :>

You entered:

        primary NTP server    : time1.google.com
        secondary NTP server  :
        secondary NTP server  :
        secondary NTP server  :
```

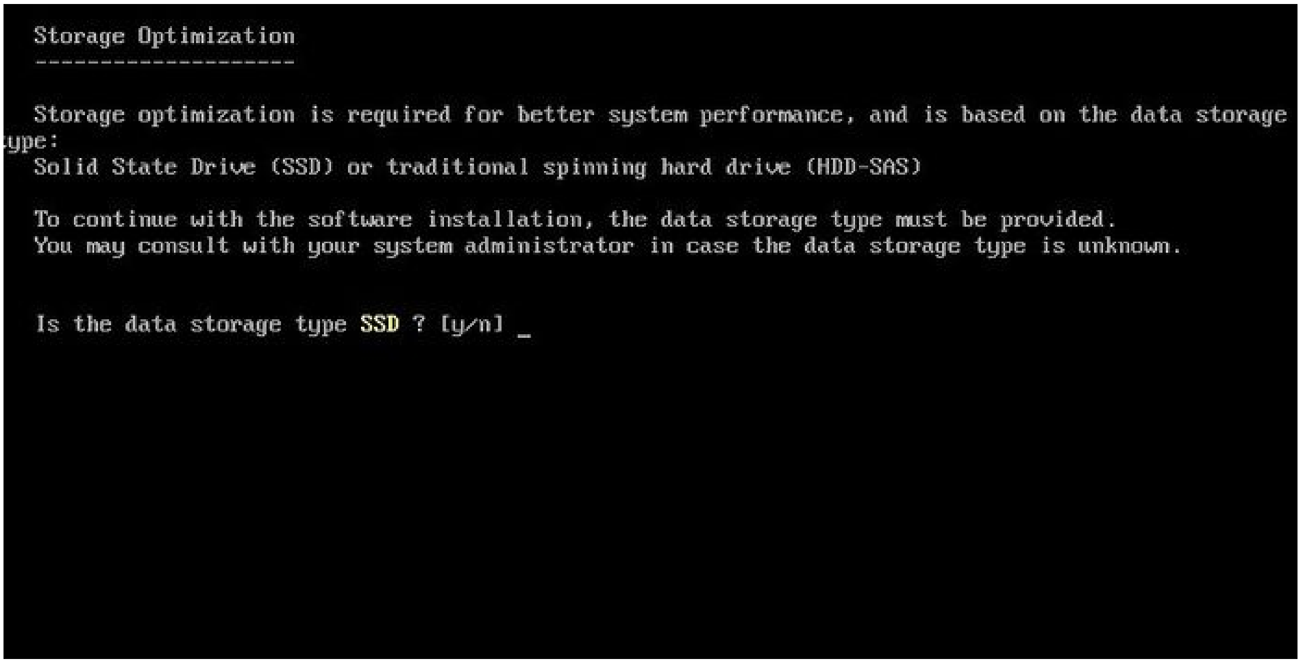
6. Choose an environment name for this DPOD installation, each DPOD installation must have a **unique** 4-character environment name

   > If you are installing a second DPOD machine that will be used as the standby machine in a DR Active/Standby scenario, the environment name must be identical to the environment name of the active DPOD installation.



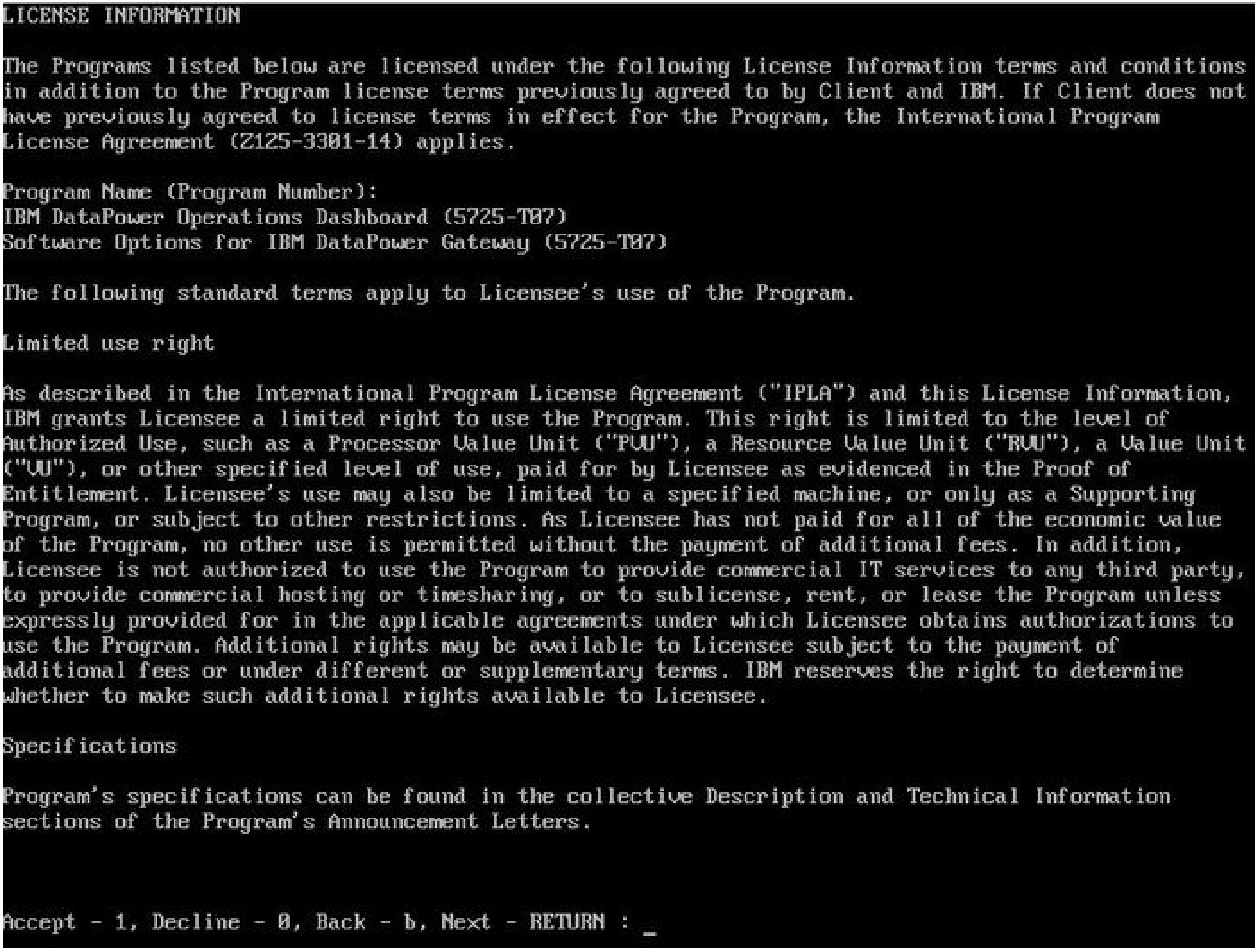
```
Installation Environment Name
------------------------------

Each installation is identified by an environment name.
Separate installations (such as prod/test/dev) must have UNIQUE environment names.
The environment name is also displayed in the Web Console.
Environment names are 4 alphanumeric characters long at most.



Please enter environment name    :>
```

7. Choose whether you use SSD storage



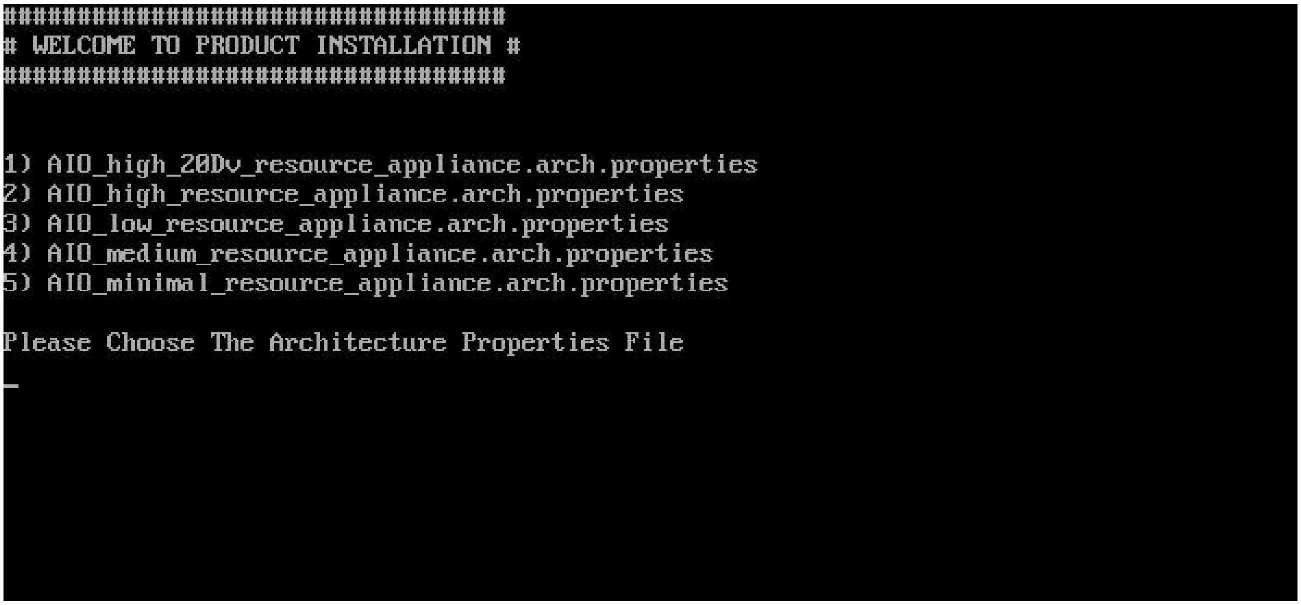
```
  Storage Optimization
  --------------------

  Storage optimization is required for better system performance, and is based on the data storage
type:
  Solid State Drive (SSD) or traditional spinning hard drive (HDD-SAS)

  To continue with the software installation, the data storage type must be provided.
  You may consult with your system administrator in case the data storage type is unknown.


  Is the data storage type SSD ? [y/n] _
```

8. Read the End User License Agreement (EULA) and if you accept the term please press 1 to accept it. You may also press 0 to decline the agreement and abort the installation.



```
LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions
in addition to the Program license terms previously agreed to by Client and IBM. If Client does not
have previously agreed to license terms in effect for the Program, the International Program
License Agreement (Z125-3301-14) applies.

Program Name (Program Number):
IBM DataPower Operations Dashboard (5725-T07)
Software Options for IBM DataPower Gateway (5725-T07)

The following standard terms apply to Licensee's use of the Program.

Limited use right

As described in the International Program License Agreement ("IPLA") and this License Information,
IBM grants Licensee a limited right to use the Program. This right is limited to the level of
Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit
("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of
Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting
Program, or subject to other restrictions. As Licensee has not paid for all of the economic value
of the Program, no other use is permitted without the payment of additional fees. In addition,
Licensee is not authorized to use the Program to provide commercial IT services to any third party,
to provide commercial hosting or timesharing, or to sublicense, rent, or lease the Program unless
expressly provided for in the applicable agreements under which Licensee obtains authorizations to
use the Program. Additional rights may be available to Licensee subject to the payment of
additional fees or under different or supplementary terms. IBM reserves the right to determine
whether to make such additional rights available to Licensee.

Specifications

Program's specifications can be found in the collective Description and Technical Information
sections of the Program's Announcement Letters.



Accept - 1, Decline - 0, Back - b, Next - RETURN : _
```

9. On the following screen, the installation program will prompt you to select an installation configuration file



```
####################################
# WELCOME TO PRODUCT INSTALLATION #
####################################


1) AIO_high_20Dv_resource_appliance.arch.properties
2) AIO_high_resource_appliance.arch.properties
3) AIO_low_resource_appliance.arch.properties
4) AIO_medium_resource_appliance.arch.properties
5) AIO_minimal_resource_appliance.arch.properties

Please Choose The Architecture Properties File
_
```

> In some special cases, DPOD's support team will send you a custom configuration file. This would be the time to FTP it to the appliance, following the instructions received from DPOD's support team.

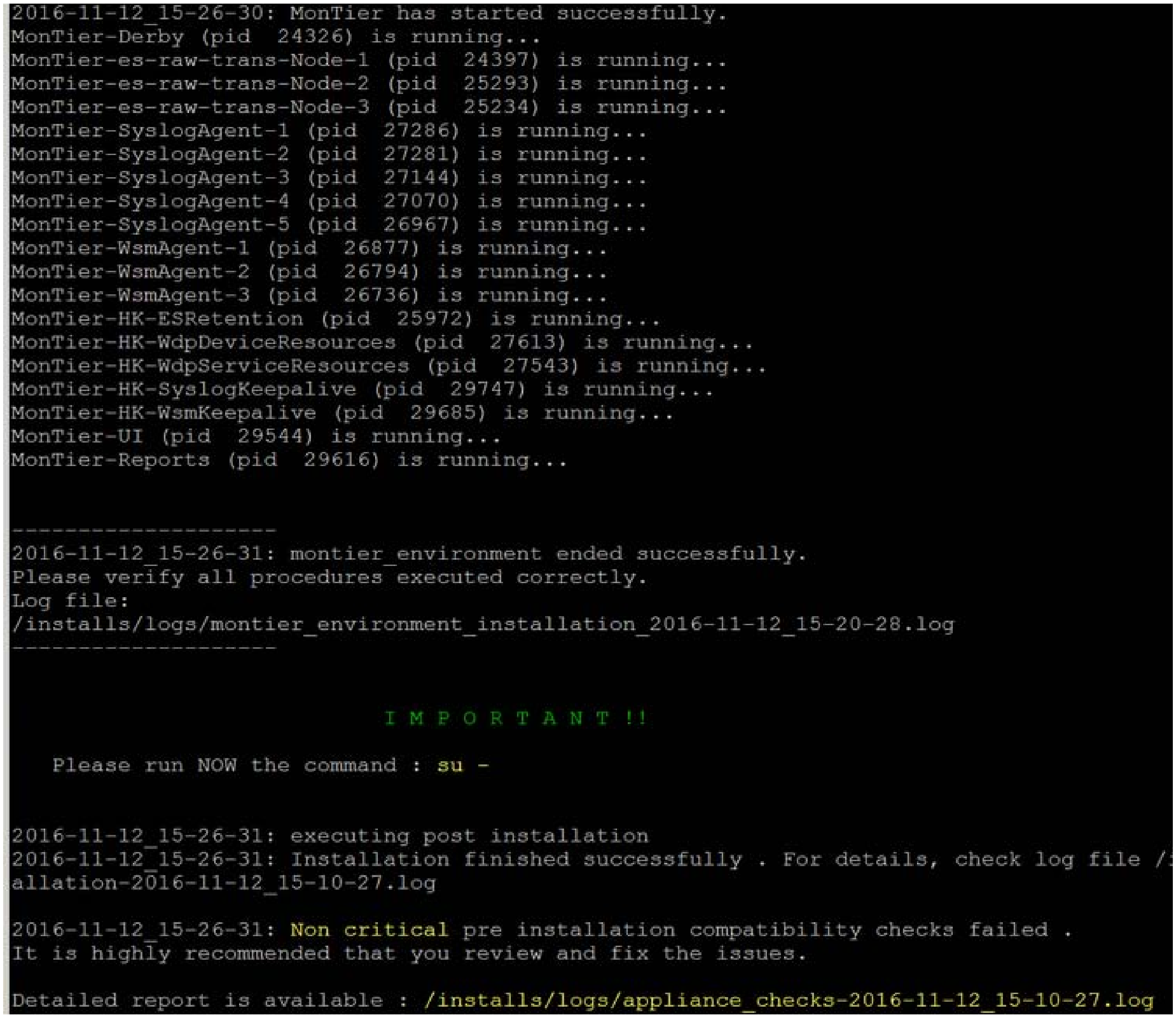
10. Select the configuration option that fits your requirements (you may consult the information found in the Hardware and Software Requirements page).
    a. Note that the list might change, and the options available to you may not match those shown above
    b. Unless otherwise instructed by DPOD Software team, use the AIO_medium_resource_appliance.arch.props
    c. If you choose to abort the installation at this stage (e.g. by using CTRL-C) and wish to start the process again at a later time, you will have to run the following command in order to undo changes and start the installation again:

       cd /app/scripts
       ./montier_env_uninstall.sh
    d. Rerun installation from step 3 but this time using the command :

```
installApp --clean
```

11. Wait for the installation to finish.
    a. Any errors will be logged to the installation log file, displayed at the end of the installation process.
    b. The /installs/logs directory contains detailed install logs for each component.

12. After displaying the messages "Stopping/Starting ...", the installation will work in silent mode - without any further messages for ~ 5 minutes, this is a normal behavior.
    When the installation is completed, you should see the following output:



```
2016-11-12_15-26-30: MonTier has started successfully.
MonTier-Derby (pid  24326) is running...
MonTier-es-raw-trans-Node-1 (pid  24397) is running...
MonTier-es-raw-trans-Node-2 (pid  25293) is running...
MonTier-es-raw-trans-Node-3 (pid  25234) is running...
MonTier-SyslogAgent-1 (pid  27286) is running...
MonTier-SyslogAgent-2 (pid  27281) is running...
MonTier-SyslogAgent-3 (pid  27144) is running...
MonTier-SyslogAgent-4 (pid  27070) is running...
MonTier-SyslogAgent-5 (pid  26967) is running...
MonTier-WsmAgent-1 (pid  26877) is running...
MonTier-WsmAgent-2 (pid  26794) is running...
MonTier-WsmAgent-3 (pid  26736) is running...
MonTier-HK-ESRetention (pid  25972) is running...
MonTier-HK-WdpDeviceResources (pid  27613) is running...
MonTier-HK-WdpServiceResources (pid  27543) is running...
MonTier-HK-SyslogKeepalive (pid  29747) is running...
MonTier-HK-WsmKeepalive (pid  29685) is running...
MonTier-UI (pid  29544) is running...
MonTier-Reports (pid  29616) is running...


--------------------
2016-11-12_15-26-31: montier_environment ended successfully.
Please verify all procedures executed correctly.
Log file:
/installs/logs/montier_environment_installation_2016-11-12_15-20-28.log
--------------------


                            I M P O R T A N T !!

   Please run NOW the command : su -


2016-11-12_15-26-31: executing post installation
2016-11-12_15-26-31: Installation finished successfully . For details, check log file /i
allation-2016-11-12_15-10-27.log

2016-11-12_15-26-31: Non critical pre installation compatibility checks failed .
It is highly recommended that you review and fix the issues.

Detailed report is available : /installs/logs/appliance_checks-2016-11-12_15-10-27.log
```

13. Login again as root or just use the "**su -"** command

```
su -
```

14. continue to Installation Verification.

Light Edition Only
Minimize Resource Consumption - In this version, **NO** special steps required to install Developer Edition as was in previous versions

Non-Appliance Installation

Perform the following steps to deploy DPOD on a Pre-installed CentOS / RHEL :

- Red Hat Enterprise Linux Server release 7.2, 7.4 , 7.5 or 7.6 (7.3 is not supported)
- CentOS version 7.2 / 7.4

Prepare the Installation files

1. Download the CEF files and move them to your appliance's /tmp directory.
   Make sure there is a minimum of 1GB available free space on /tmp directory after you copied the CEF file.
   You can execute the CEF file from another directory or alternatively, instruct the CEF file to extract to different directory using the command option --dest-dir <directory path>

2. Run *chmod 755* on the files

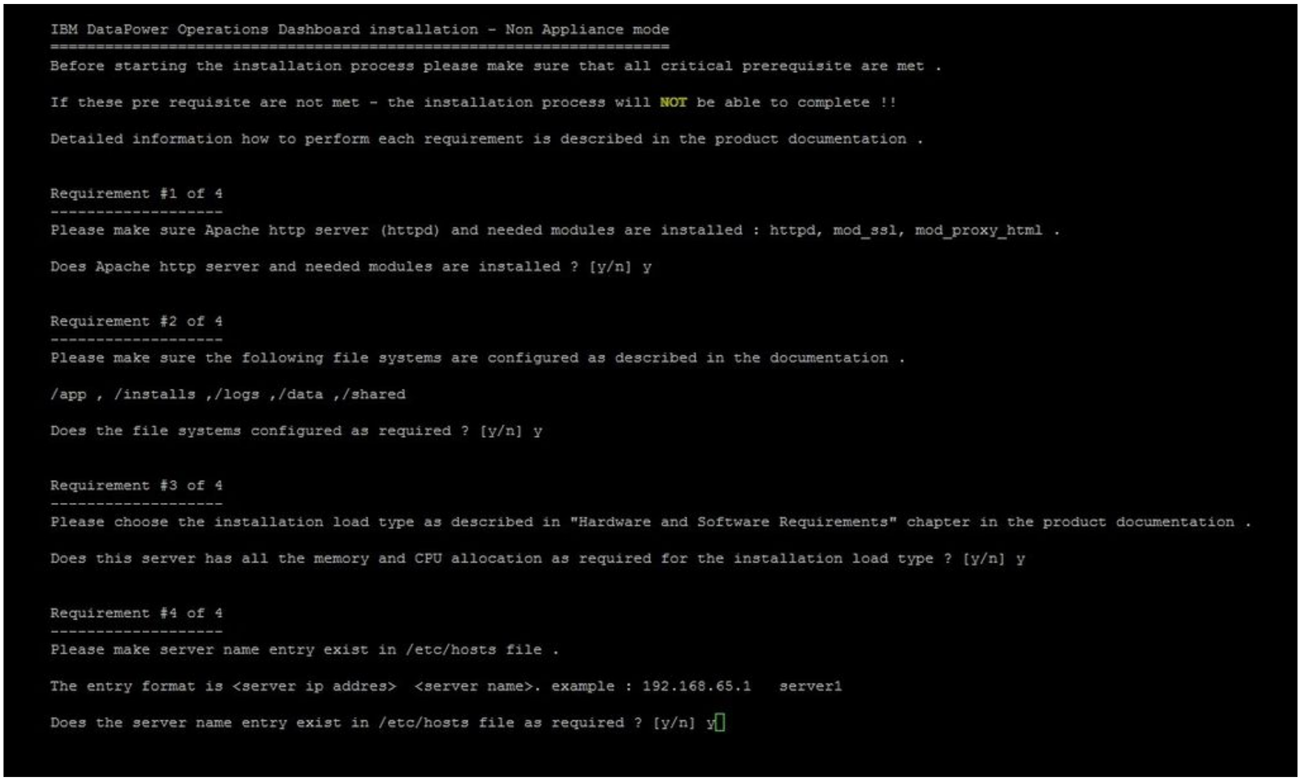
Execute the CEF File

1. From the location of the CEF file, execute the CEF (the CEF file is in a Compressed Executable Format)

   For example, if the file name is DPOD-version-1.cef – run *./DPOD-version-1.cef*

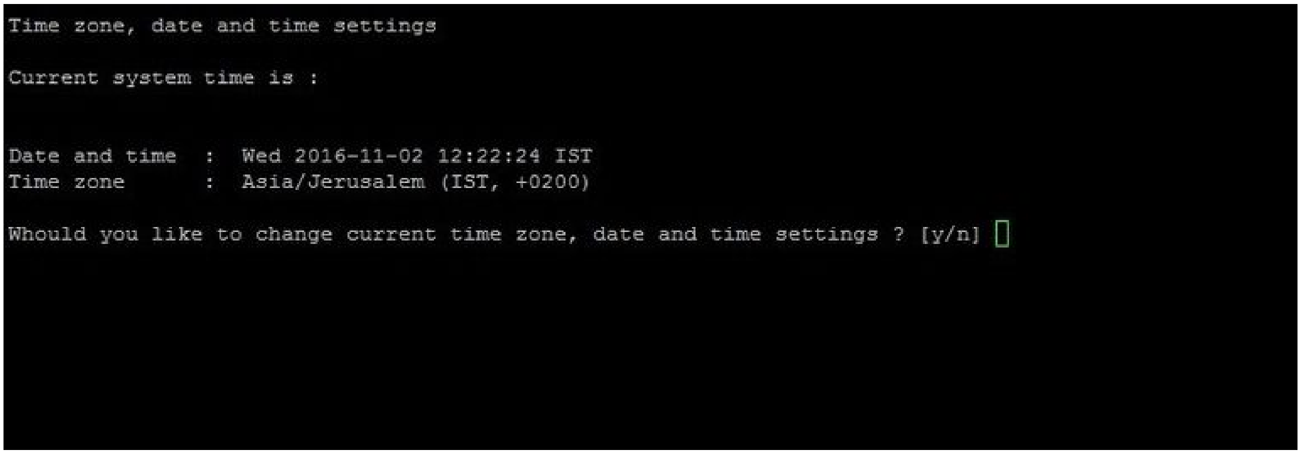
The Installation Process

1. The CEF installer displays a series of questions, requiring you to verify that your appliance meets the installation prerequisites



```
IBM DataPower Operations Dashboard installation - Non Appliance mode
====================================================================
Before starting the installation process please make sure that all critical prerequisite are met .

If these pre requisite are not met - the installation process will NOT be able to complete !!

Detailed information how to perform each requirement is described in the product documentation .


Requirement #1 of 4
-------------------
Please make sure Apache http server (httpd) and needed modules are installed : httpd, mod_ssl, mod_proxy_html .

Does Apache http server and needed modules are installed ? [y/n] y


Requirement #2 of 4
-------------------
Please make sure the following file systems are configured as described in the documentation .

/app , /installs ,/logs ,/data ,/shared

Does the file systems configured as required ? [y/n] y


Requirement #3 of 4
-------------------
Please choose the installation load type as described in "Hardware and Software Requirements" chapter in the product documentation .

Does this server has all the memory and CPU allocation as required for the installation load type ? [y/n] y


Requirement #4 of 4
-------------------
Please make server name entry exist in /etc/hosts file .

The entry format is <server ip addres>  <server name>. example : 192.168.65.1   server1

Does the server name entry exist in /etc/hosts file as required ? [y/n] y
```

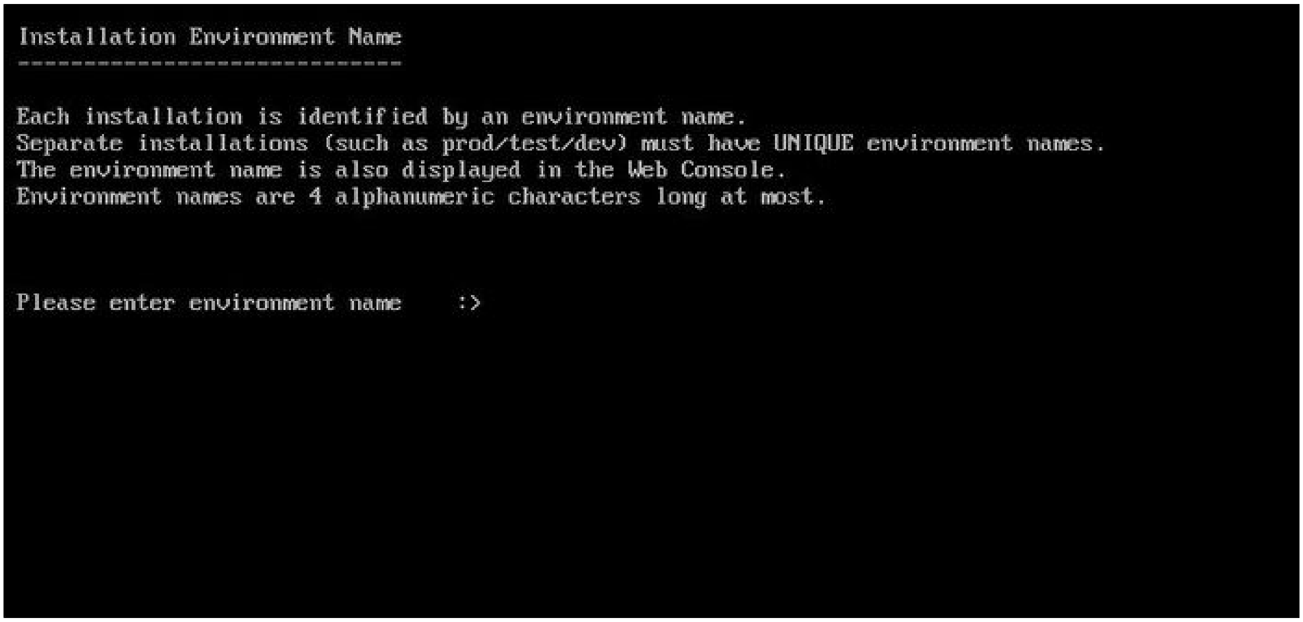
2. Once you answered Yes to all questions, the installer will verify the system meets all prerequisites
3. Next, you can change the time and date settings (or leave them as they are)



```
Time zone, date and time settings

Current system time is :


Date and time   :  Wed 2016-11-02 12:22:24 IST
Time zone       :  Asia/Jerusalem (IST, +0200)

Whould you like to change current time zone, date and time settings ? [y/n]
```

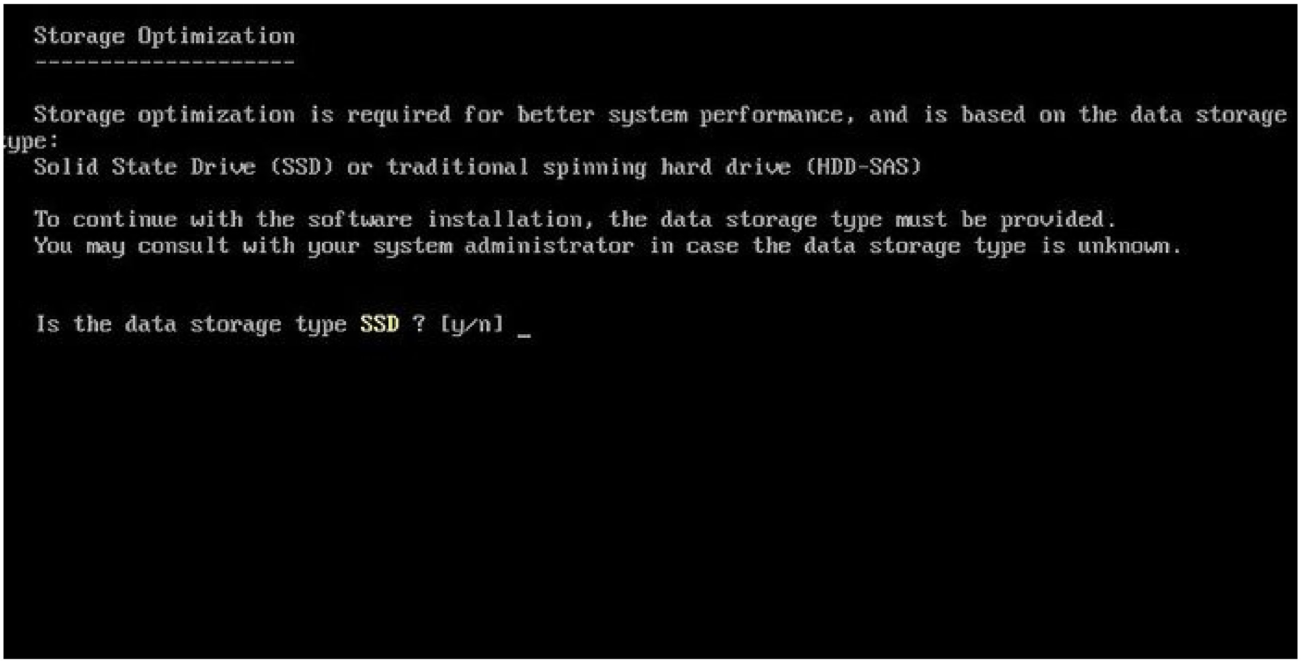
4. Choose an environment name for this DPOD installation, each DPOD installation must have a **unique** 4-character environment name

> If you are installing a second DPOD machine that will be used as the standby machine in a DR Active/Standby scenario, the environment name must be identical to the environment name of the active DPOD installation.



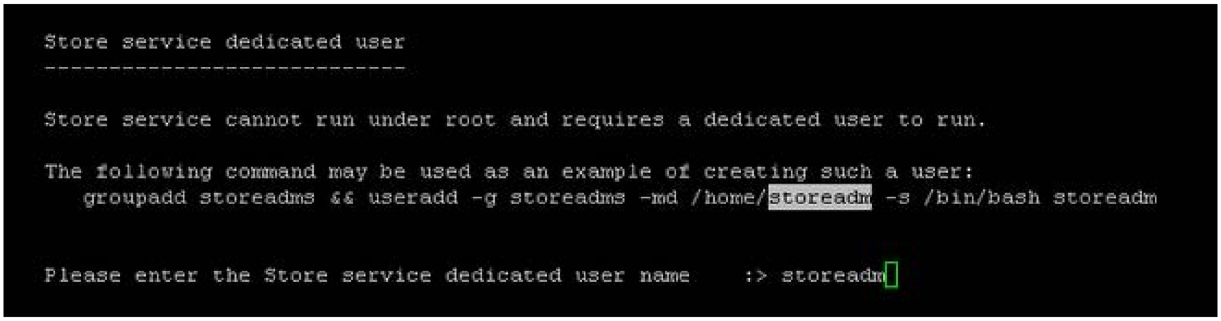
```
Installation Environment Name
-----------------------------

Each installation is identified by an environment name.
Separate installations (such as prod/test/dev) must have UNIQUE environment names.
The environment name is also displayed in the Web Console.
Environment names are 4 alphanumeric characters long at most.



Please enter environment name    :>
```

5. Choose whether you use SSD storage



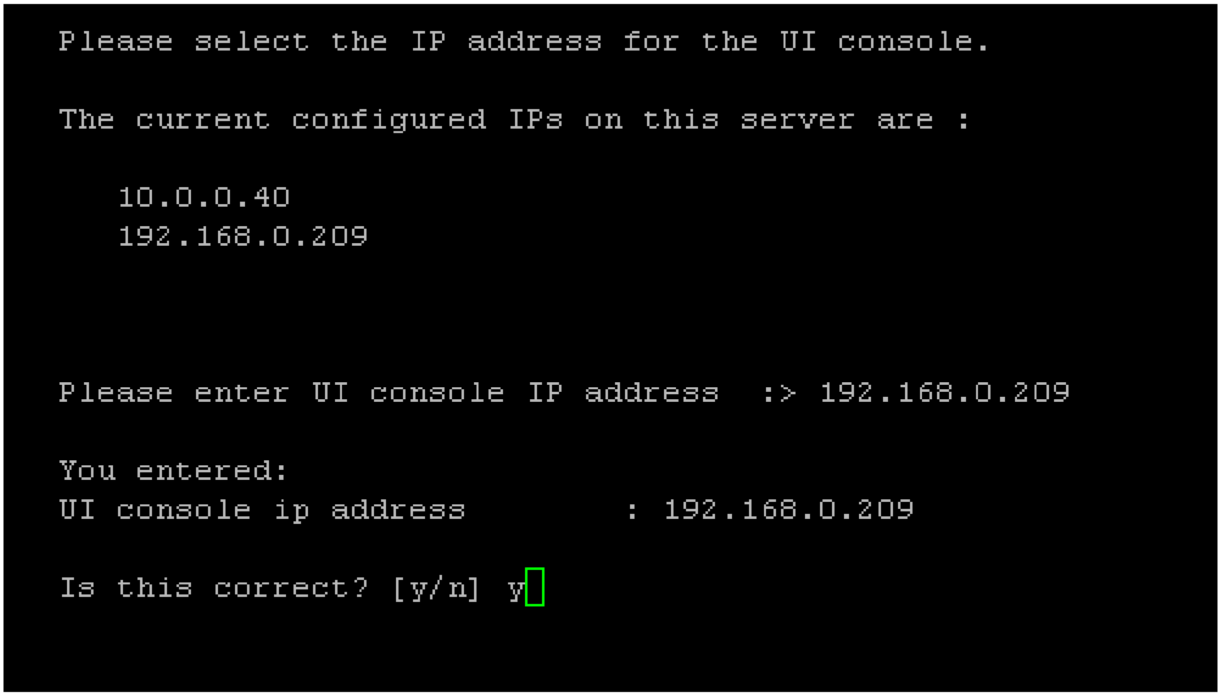
```
  Storage Optimization
  --------------------

  Storage optimization is required for better system performance, and is based on the data storage
type:
  Solid State Drive (SSD) or traditional spinning hard drive (HDD-SAS)

  To continue with the software installation, the data storage type must be provided.
  You may consult with your system administrator in case the data storage type is unknown.


  Is the data storage type SSD ? [y/n] _
```

6. Set Store Service dedicated user



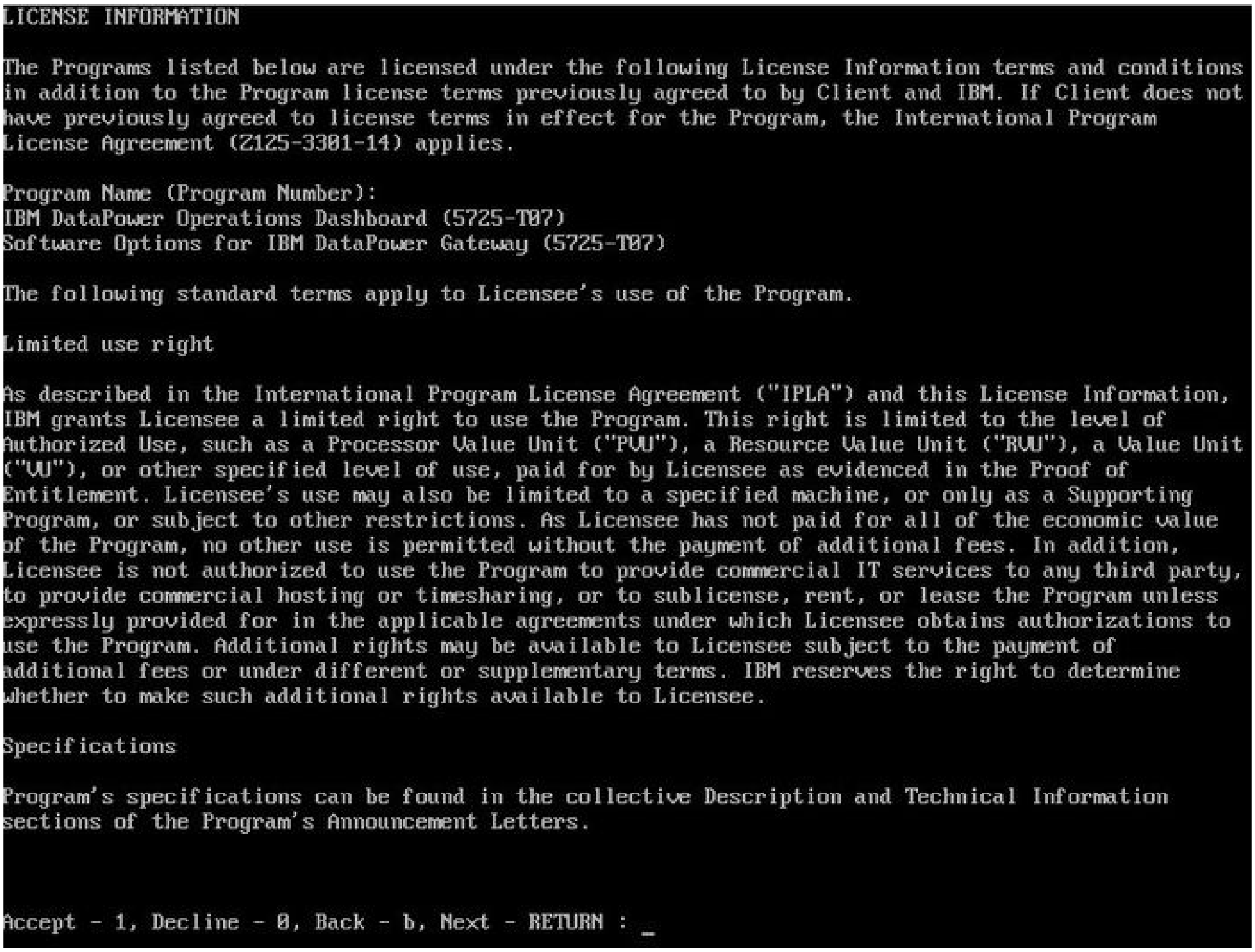
```
Store service dedicated user
----------------------------

Store service cannot run under root and requires a dedicated user to run.

The following command may be used as an example of creating such a user:
   groupadd storeadms && useradd -g storeadms -md /home/storeadm -s /bin/bash storeadm


Please enter the Store service dedicated user name     :> storeadm
```

7. (Optional) If you have 2 NIC than this question may appear :



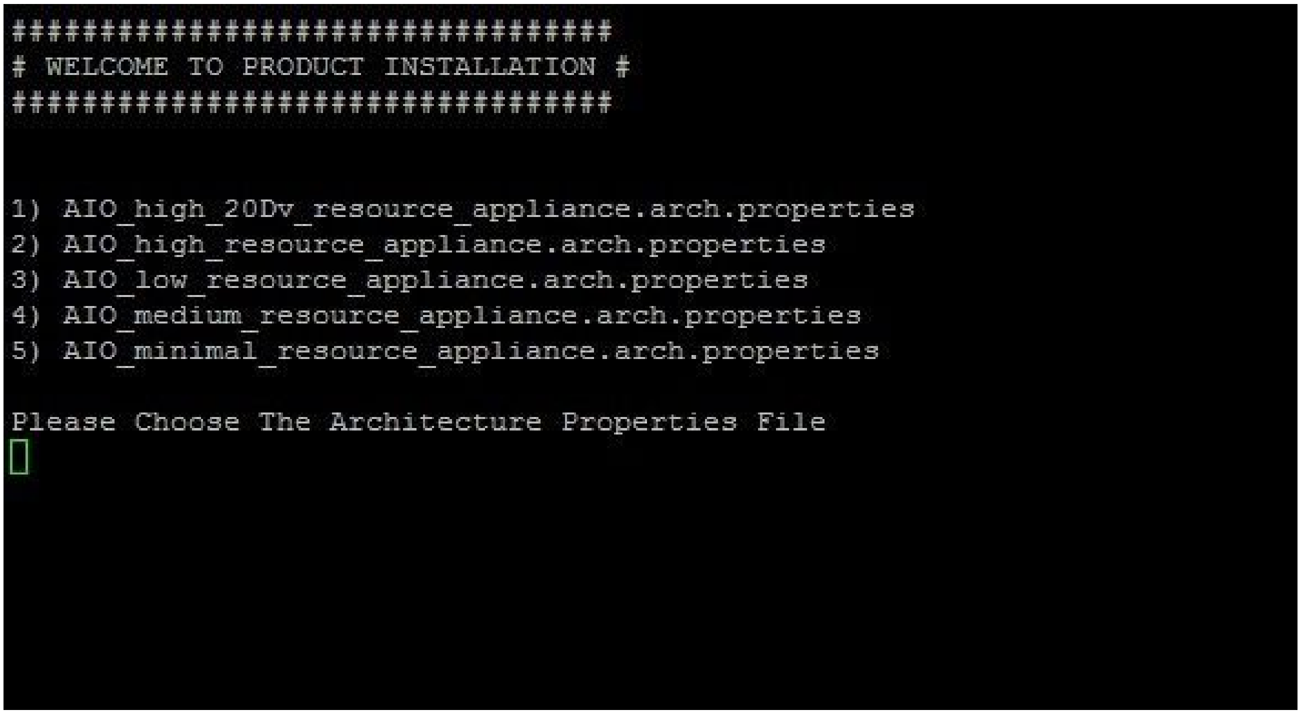
```
Please select the IP address for the UI console.

The current configured IPs on this server are :

   10.0.0.40
   192.168.0.209



Please enter UI console IP address   :> 192.168.0.209

You entered:
UI console ip address          : 192.168.0.209

Is this correct? [y/n] y
```

8. Accept or Decline the EULA



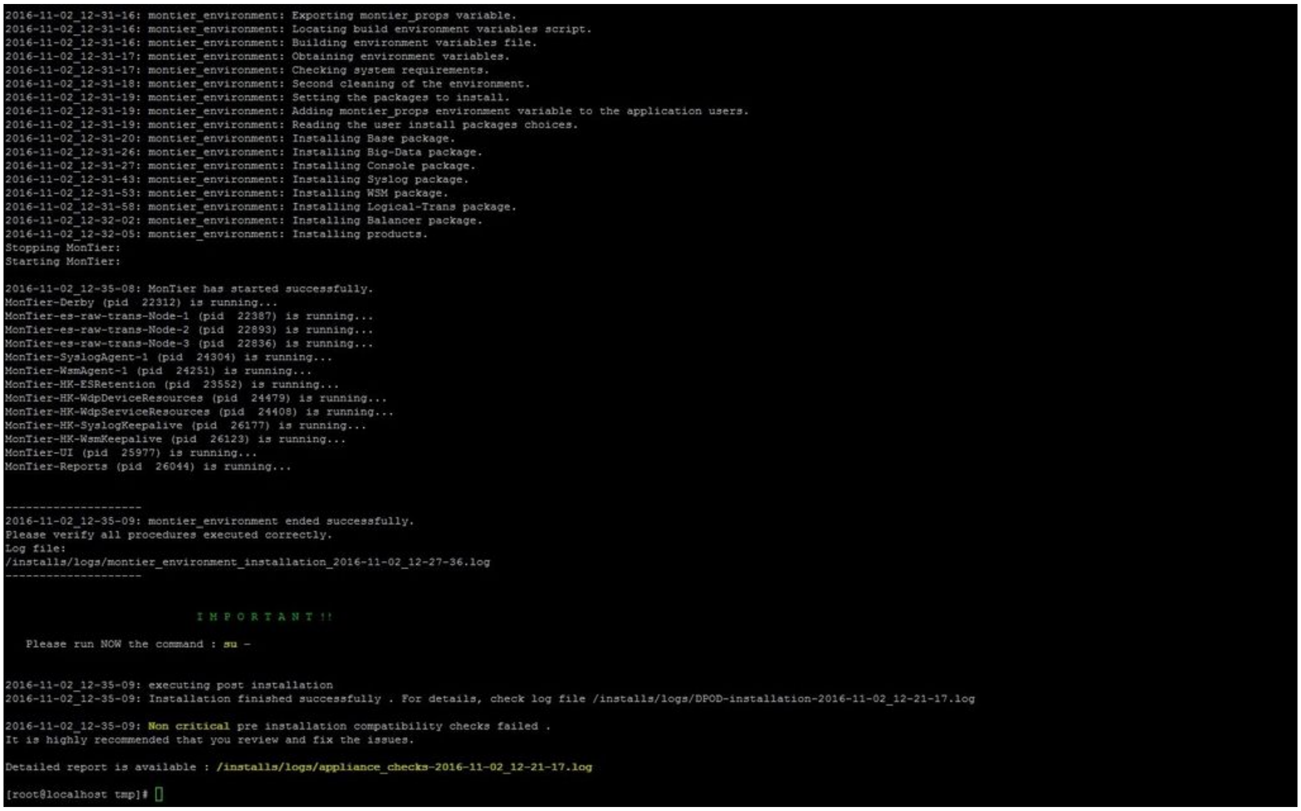
```
LICENSE INFORMATION

The Programs listed below are licensed under the following License Information terms and conditions
in addition to the Program license terms previously agreed to by Client and IBM. If Client does not
have previously agreed to license terms in effect for the Program, the International Program
License Agreement (Z125-3301-14) applies.

Program Name (Program Number):
IBM DataPower Operations Dashboard (5725-T07)
Software Options for IBM DataPower Gateway (5725-T07)

The following standard terms apply to Licensee's use of the Program.

Limited use right

As described in the International Program License Agreement ("IPLA") and this License Information,
IBM grants Licensee a limited right to use the Program. This right is limited to the level of
Authorized Use, such as a Processor Value Unit ("PVU"), a Resource Value Unit ("RVU"), a Value Unit
("VU"), or other specified level of use, paid for by Licensee as evidenced in the Proof of
Entitlement. Licensee's use may also be limited to a specified machine, or only as a Supporting
Program, or subject to other restrictions. As Licensee has not paid for all of the economic value
of the Program, no other use is permitted without the payment of additional fees. In addition,
Licensee is not authorized to use the Program to provide commercial IT services to any third party,
to provide commercial hosting or timesharing, or to sublicense, rent, or lease the Program unless
expressly provided for in the applicable agreements under which Licensee obtains authorizations to
use the Program. Additional rights may be available to Licensee subject to the payment of
additional fees or under different or supplementary terms. IBM reserves the right to determine
whether to make such additional rights available to Licensee.

Specifications

Program's specifications can be found in the collective Description and Technical Information
sections of the Program's Announcement Letters.



Accept - 1, Decline - 0, Back - b, Next - RETURN : _
```

9. Choose the installation architecture, Ensure your appliance has enough memory and storage available, or the installation will stop
   The Architecture options you see on-screen may differ from the ones in the screenshot below, as they depend on the installation package you obtained.



```
####################################
# WELCOME TO PRODUCT INSTALLATION #
####################################


1) AIO_high_20Dv_resource_appliance.arch.properties
2) AIO_high_resource_appliance.arch.properties
3) AIO_low_resource_appliance.arch.properties
4) AIO_medium_resource_appliance.arch.properties
5) AIO_minimal_resource_appliance.arch.properties

Please Choose The Architecture Properties File
```

10. The installation will commence. The process takes 5-15 minutes, and when it ends the installer displays a message indicating whether the process was successful or not,
    alongside the name of the installation log file



```
2016-11-02_12-31-16: montier_environment: Exporting montier_props variable.
2016-11-02_12-31-16: montier_environment: Locating build environment variables script.
2016-11-02_12-31-16: montier_environment: Building environment variables file.
2016-11-02_12-31-17: montier_environment: Obtaining environment variables.
2016-11-02_12-31-17: montier_environment: Checking system requirements.
2016-11-02_12-31-18: montier_environment: Second cleaning of the environment.
2016-11-02_12-31-19: montier_environment: Setting the packages to install.
2016-11-02_12-31-19: montier_environment: Adding montier_props environment variable to the application users.
2016-11-02_12-31-19: montier_environment: Reading the user install packages choices.
2016-11-02_12-31-20: montier_environment: Installing Base package.
2016-11-02_12-31-26: montier_environment: Installing Big-Data package.
2016-11-02_12-31-27: montier_environment: Installing Console package.
2016-11-02_12-31-43: montier_environment: Installing Syslog package.
2016-11-02_12-31-53: montier_environment: Installing WSM package.
2016-11-02_12-31-58: montier_environment: Installing Logical-Trans package.
2016-11-02_12-32-02: montier_environment: Installing Balancer package.
2016-11-02_12-32-05: montier_environment: Installing products.
Stopping MonTier:
Starting MonTier:

2016-11-02_12-35-08: MonTier has started successfully.
MonTier-Derby (pid  22312) is running...
MonTier-es-raw-trans-Node-1 (pid  22387) is running...
MonTier-es-raw-trans-Node-2 (pid  22893) is running...
MonTier-es-raw-trans-Node-3 (pid  22836) is running...
MonTier-SyslogAgent-1 (pid  24304) is running...
MonTier-WsmAgent-1 (pid  24251) is running...
MonTier-HK-ESRetention (pid  23552) is running...
MonTier-HK-WdpDeviceResources (pid  24479) is running...
MonTier-HK-WdpServiceResources (pid  24408) is running...
MonTier-HK-SyslogKeepalive (pid  26177) is running...
MonTier-HK-WsmKeepalive (pid  26123) is running...
MonTier-UI (pid  25977) is running...
MonTier-Reports (pid  26044) is running...


--------------------
2016-11-02_12-35-09: montier_environment ended successfully.
Please verify all procedures executed correctly.
Log file:
/installs/logs/montier_environment_installation_2016-11-02_12-27-36.log
--------------------


                           I M P O R T A N T !!

   Please run NOW the command : su -


2016-11-02_12-35-09: executing post installation
2016-11-02_12-35-09: Installation finished successfully . For details, check log file /installs/logs/DPOD-installation-2016-11-02_12-21-17.log

2016-11-02_12-35-09: Non critical pre installation compatibility checks failed .
It is highly recommended that you review and fix the issues.

Detailed report is available : /installs/logs/appliance_checks-2016-11-02_12-21-17.log

[root@localhost tmp]#
```

11. Verify your installation

Installation Verification

When you have completed the tasks in Appliance Installation and Software Deployment, you should verify that DPOD installed correctly. Follow the steps below to complete the verification process.

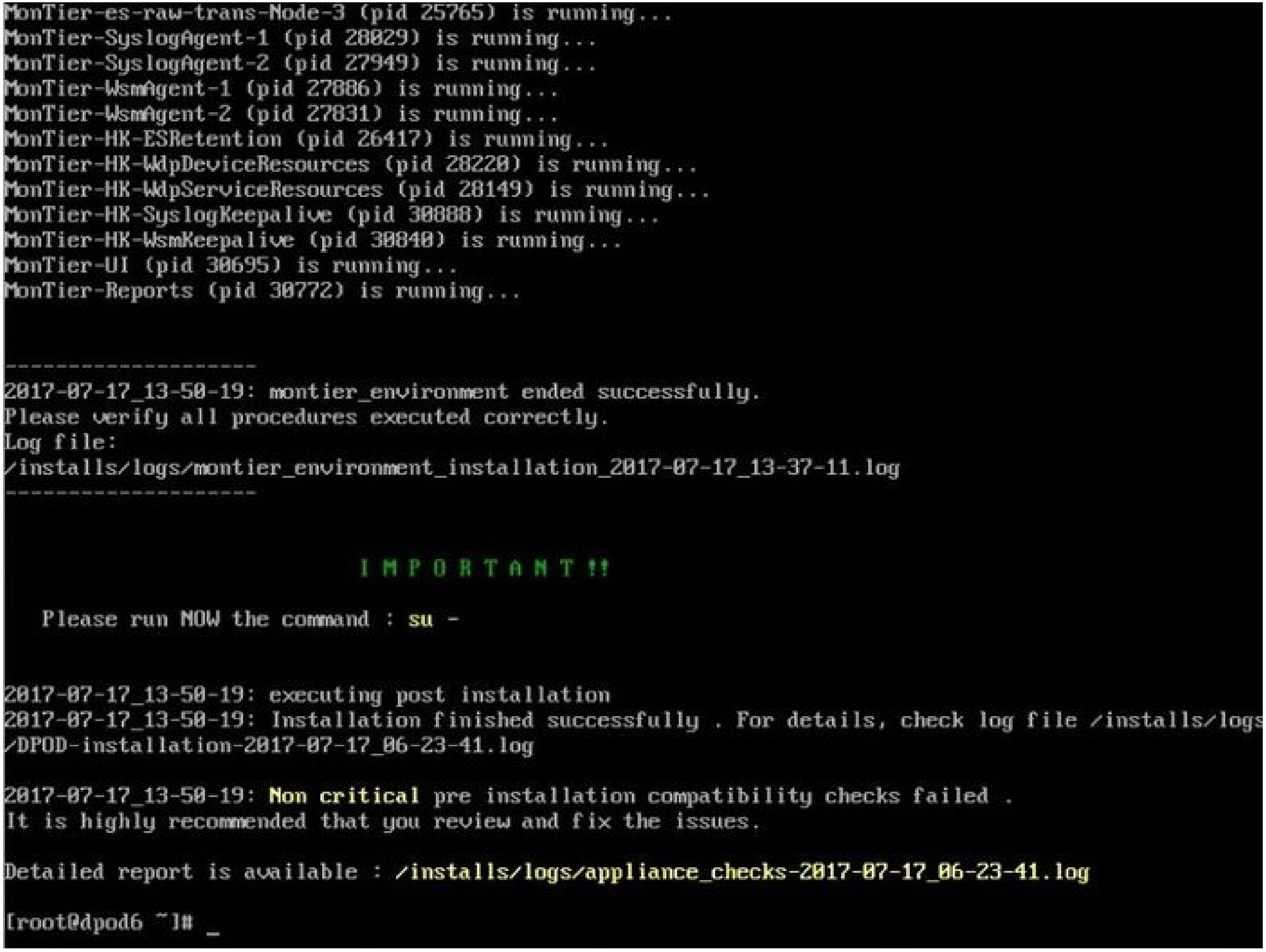
1. Verify that there are no errors in the installation logs, as described in Handling Installations Errors
2. Start the admin CLI and check the system services status
3. While at the admin CLI, Stop all system services
4. Verify that all services are down.
5. Start All System Services
6. Verify all services are in running state.

After completing these verification steps with no errors

- Your installation is verified
- Your system is up and running

HANDLING INSTALLATION ERRORS

After the Software Deployment task is completed, the system displays the following screen:



```
MonTier-es-raw-trans-Node-3 (pid 25765) is running...
MonTier-SyslogAgent-1 (pid 28829) is running...
MonTier-SyslogAgent-2 (pid 27949) is running...
MonTier-WsmAgent-1 (pid 27886) is running...
MonTier-WsmAgent-2 (pid 27831) is running...
MonTier-HK-ESRetention (pid 26417) is running...
MonTier-HK-WdpDeviceResources (pid 28220) is running...
MonTier-HK-WdpServiceResources (pid 28149) is running...
MonTier-HK-SyslogKeepalive (pid 30888) is running...
MonTier-HK-WsmKeepalive (pid 30840) is running...
MonTier-UI (pid 30695) is running...
MonTier-Reports (pid 30772) is running...


--------------------
2017-07-17_13-50-19: montier_environment ended successfully.
Please verify all procedures executed correctly.
Log file:
/installs/logs/montier_environment_installation_2017-07-17_13-37-11.log
--------------------


                             I M P O R T A N T !!

   Please run NOW the command : su -


2017-07-17_13-50-19: executing post installation
2017-07-17_13-50-19: Installation finished successfully . For details, check log file /installs/logs
/DPOD-installation-2017-07-17_06-23-41.log

2017-07-17_13-50-19: Non critical pre installation compatibility checks failed .
It is highly recommended that you review and fix the issues.

Detailed report is available : /installs/logs/appliance_checks-2017-07-17_06-23-41.log

[root@dpod6 ~]# _
```

If the installation completed unsuccessfully, the screen shows an indication that errors occurred, and asks the user to consult the installation log file. (The path to the installation log file is displayed at the end of the output).
The error displayed will read **"There was a problem installing one or more of the packages <location of the log file>"**

To investigate the error, open the file and search for an error string. Error messages direct you to specific component logs, where detailed information about the errors and resolution are available.

> All installation logs are located in /install/logs.

Data Migration Procedure

This procedure is intended for users who want to migrate from one DPOD installation to another for the following scenarios:

- Migration from DPOD Appliance mode installation version v1.0.0 with CentOS 6.7 to CentOS 7.2 introduced at version v1.0.2+.
- Migration from DPOD on a virtual server to physical server (e.g when load increased and requires a physical server based installation).
- Migration from DPOD Appliance to Non-Appliance mode (RHEL) to better comply with the organization's technical / security requirements and standards.

New procedure and tools were introduced to support customers with migration of an existing DPOD Store data to a new DPOD installation in each of the scenarios above.

The procedure includes the following main steps :

- Gather required artifacts from current (migrate from) DPOD installation.
- Install new DPOD "clean" installation.
- Import artifacts to the new DPOD installation.

Pre Requisites

- Both systems (current and new) must be with the same DPOD version, 1.0.6.0 and above.

> We highly recommend to contact DPOD support during the planing of migration in order to verify the technical procedure.

COLLECT REQUIRED ARTIFACTS FROM SOURCE SYSTEM

Application Files and Internal DB

Invoke the backup command

```
app_backup.sh
INFO : backup finished successfully. for more information see log file
/installs/system-backup/full-backup-2017-09-11_17-17-59/full-backup-2017
-09-11_17-17-59.log
```

The output backup directory will be the location of the backup log as printed in the backup status message (in the example above this is /installs/system-backup/full-backup-2017-09-11_17-17-59).

Copy the backup directory to a temporary location outside the current DPOD system.

Services Files

DPOD's service files are located in the /etc/init.d directory

The service files will not be migrated to the new system because they are not compatible with the new OS version.

If the user altered one of the service files manually, it is their responsibility to migrate these changes to the new service files.

User Custom Artifacts

> If the user is using any custom artifacts which are NOT located in one of the system builtin locations, it is the customer's responsibility to migrate these artifacts from the current system to the new one.

Examples of custom artifacts include custom key stores used for DPOD SSL client authentication.

CREATING NEW SYSTEM

Install new System

Install a new DPOD system using version 1.0.2.0 ISO file and apply needed updates (fix) in order for the the current system and the new system to have the same DPOD version.

Disable Log Targets

Since DPOD will not be available during the migration process we recommend to disable the monitored device's log targets on the current (old) DPOD installation as describe in "Disable / Enable DPOD's Log Targets".

Move The Data Disk - Optional

The current transactions data is stored in the BigData store located on the OS mount point /data .

> It is not mandatory to migrate the current transaction data to the new system.
>
> Not migrating the transaction data means losing current transaction data!

To migrate the current transactions data to the new system please follow the procedure below.

If you choose NOT to migrate transaction data (only configuration data) skip to "Create Staging Directory"

> All technical names in the following section are used in DPOD Appliance mode installation.
>
> If the user installation is Non Appliance RHEL installation the technical name may be different (based on the organizational standard). Please contact your system administrator.

Exporting The Data LVM Configuration (Volume Group) On The Source Installation

The /data mount point is mapped to the LVM volume group vg_data

- Stop the application services using the Main Admin Menu CLI (option 2 "stop all")
- un-mount the /data mount point

```
umount /data
```

- Mark the volume group as non active

```
vgchange -an vg_data
output : 0 logical volume(s) in volume group "vg_data" now active
```

- Export the volume group

```
vgexport vg_data
output : Volume group "vg_data" successfully exported
```

- Comment /data mount point in OS FS table

Comment the following line in /etc/fstab

```
#/dev/mapper/vg_data-lv_data /data                   ext4
defaults        1 2
```

Disconnect the Data Disk and Connect to the New System

Stop The System

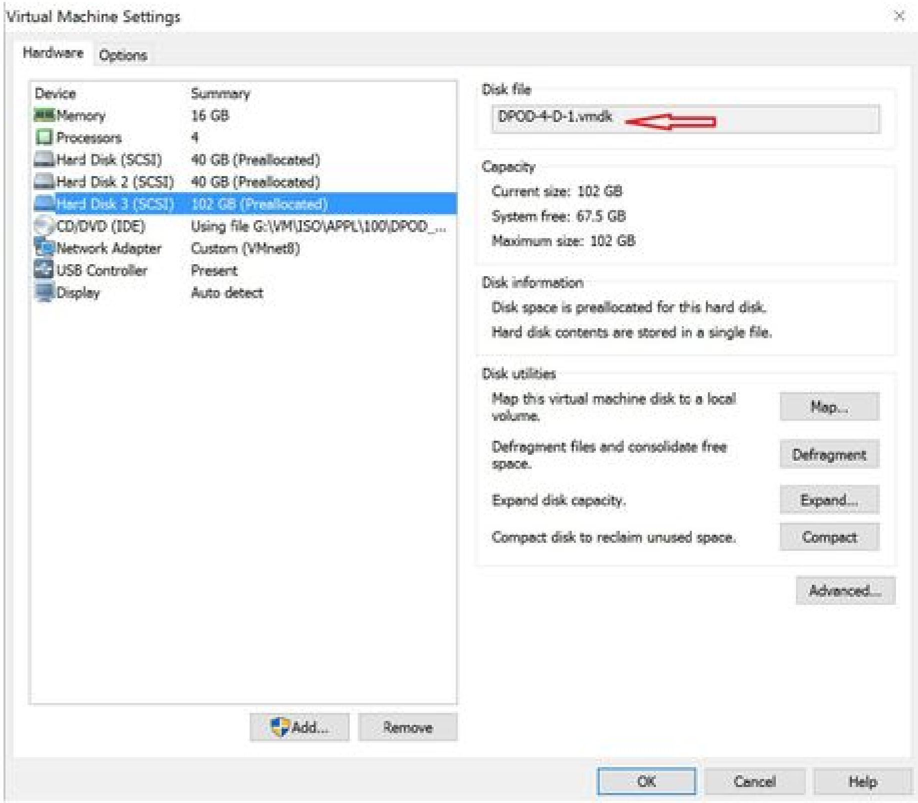
shutdown the server (virtual / physical) using the command

```
shutdown -h 0
```

Virtual Environment

Copy the Virtual Data Disk From the Current VM

- Edit the current virtual machine settings
- Locate the data disk (hard drive number 3)
- It is recommended to copy the data disk vmdk file to the new system directory (we recommend NOT to move the vmdk file but copy it, in order to retain a fallback option in case of an issue during migration).



Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	40 GB (Preallocated)
Hard Disk 2 (SCSI)	40 GB (Preallocated)
Hard Disk 3 (SCSI)	102 GB (Preallocated)
CD/DVD (IDE)	Using file G:\VM\ISO\APPL\100\DPOD_...
Network Adapter	Custom (VMnet8)
USB Controller	Present
Display	Auto detect

Disk file

DPOD-4-D-1.vmdk

Capacity

Current size: 102 GB

System free: 67.5 GB

Maximum size: 102 GB

Disk information

Disk space is preallocated for this hard disk.

Hard disk contents are stored in a single file.

Disk utilities

Map this virtual machine disk to a local volume.

Defragment files and consolidate free space.

Expand disk capacity.

Compact disk to reclaim unused space.

Edit the New System OS FS table

Change the /data mount point in OS FS table

```
From : /dev/mapper/vg_data-lv_data /data                      xfs
defaults        0 0
To   : /dev/mapper/vg_data_old-lv_data /data                  xfs
defaults        0 0
```

Rename /data LVM volume Group

Rename the data volume group vg_data in the new system to avoid volume group collision when connecting the data disk from the old system

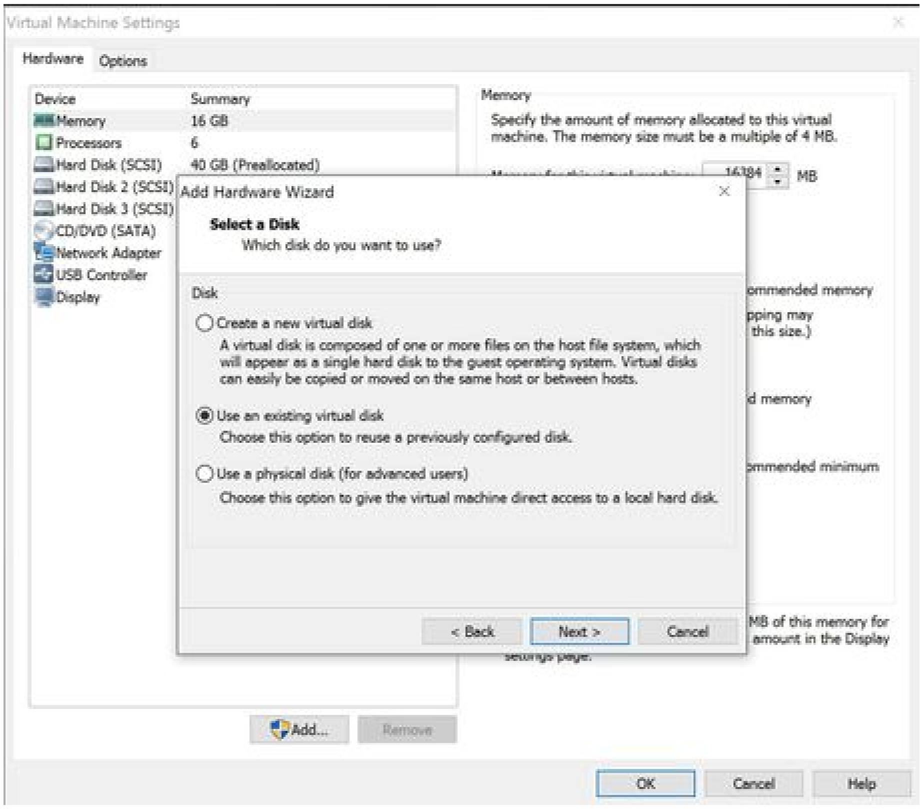
```
vgrename vg_data vg_data_old

output : Volume group "vg_data" successfully renamed to "vg_data_old"
```

Connect the Virtual Disk to New VM

- Shut down the new system

```
shutdown -h 0
```

- Configure the virtual disk on the new system by adding a new hard drive and choosing existing



Device	Summary
Memory	16 GB
Processors	6
Hard Disk (SCSI)	40 GB (Preallocated)
Hard Disk 2 (SCSI)	
Hard Disk 3 (SCSI)	
CD/DVD (SATA)	
Network Adapter	
USB Controller	
Display	

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

16384 MB

Select a Disk

Which disk do you want to use?

Disk

○ Create a new virtual disk

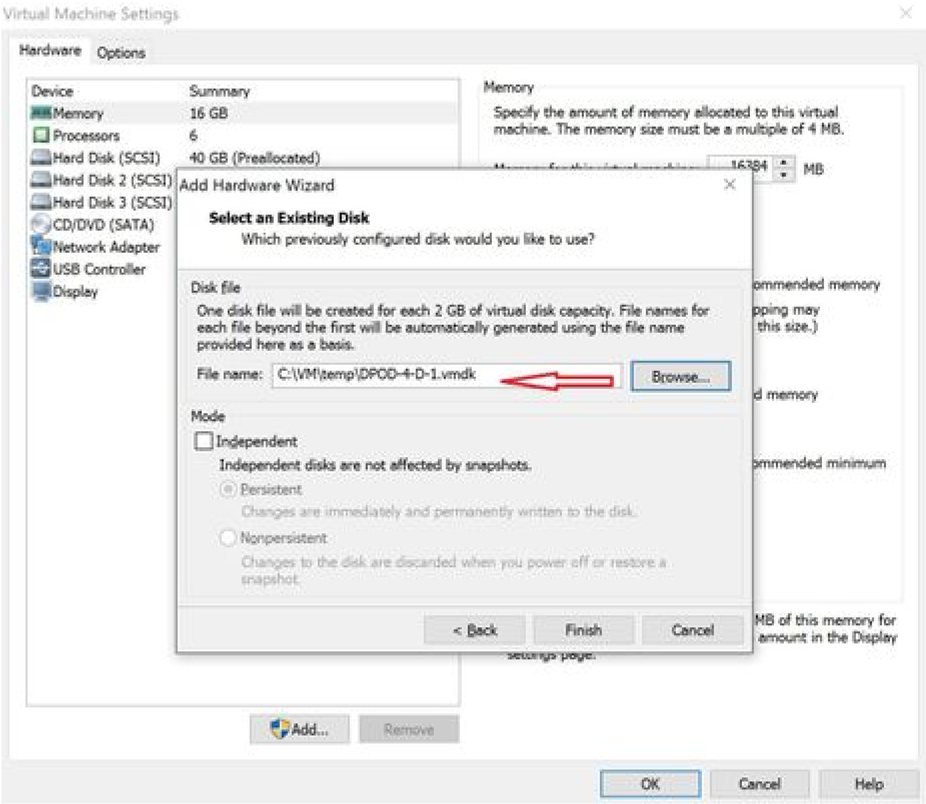
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

● Use an existing virtual disk

Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk.



Virtual Machine Settings

Hardware Options

Device	Summary
Memory	16 GB
Processors	6
Hard Disk (SCSI)	40 GB (Preallocated)
Hard Disk 2 (SCSI)	
Hard Disk 3 (SCSI)	
CD/DVD (SATA)	
Network Adapter	
USB Controller	
Display	

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

16384 MB

Add Hardware Wizard

Select an Existing Disk

Which previously configured disk would you like to use?

Disk file

One disk file will be created for each 2 GB of virtual disk capacity. File names for each file beyond the first will be automatically generated using the file name provided here as a basis.

File name: C:\VM\temp\DPOD-4-D-1.vmdk

Mode

□ Independent

Independent disks are not affected by snapshots.

● Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to the disk are discarded when you power off or restore a snapshot.

- Start the new VM

Configure the New Disk

- Make sure the new exported volume group (LVM vg) and physical volume (LVM pv) are recognized by the OS

```
pvscan
output :
  PV /dev/sdb3   VG vg_app        lvm2 [7.08 GiB / 80.00 MiB free]
  PV /dev/sdb1   VG vg_logs       lvm2 [11.08 GiB / 84.00 MiB free]
  PV /dev/sdb5   VG vg_apptmp     lvm2 [4.10 GiB / 100.00 MiB free]
  PV /dev/sdb6   VG vg_shared     lvm2 [596.00 MiB / 84.00 MiB free]
  PV /dev/sdd1    is in exported VG vg_data [101.97 GiB / 0    free]
  PV /dev/sda2   VG vg_root       lvm2 [10.19 GiB / 196.00 MiB free]
  PV /dev/sdb2   VG vg_inst       lvm2 [7.08 GiB / 80.00 MiB free]
  PV /dev/sdc1   VG vg_data_old   lvm2 [100.00 GiB / 20.00 MiB free]
  Total: 8 [242.07 GiB] / in use: 8 [242.07 GiB] / in no VG: 0 [0   ]
```

```
vgscan
output :
  Reading all physical volumes.  This may take a while...
  Found volume group "vg_data_old" using metadata type lvm2
  Found volume group "vg_inst" using metadata type lvm2
  Found volume group "vg_root" using metadata type lvm2
  Found exported volume group "vg_data" using metadata type lvm2
  Found volume group "vg_shared" using metadata type lvm2
  Found volume group "vg_apptmp" using metadata type lvm2
  Found volume group "vg_logs" using metadata type lvm2
  Found volume group "vg_app" using metadata type lvm2
```

- Import the data volume group from the new disk added to VM

```
vgimport vg_data

output :
  Volume group "vg_data" successfully imported
```

- Activate the imported data volume group

```
vgimport vg_data

output :
   1 logical volume(s) in volume group "vg_data" now active
```

- Verify the data volume group status

```
vgdisplay vg_data

output :
   --- Volume group ---
  VG Name               vg_data
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  4
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                1
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               101.97 GiB
  PE Size               32.00 MiB
  Total PE              3263
  Alloc PE / Size       3263 / 101.97 GiB
  Free  PE / Size       0 / 0
  VG UUID               4vIe7h-qqLR-6qEa-aRID-dU8w-U5E2-gV7FoJ
```

Add the new mount point to the OS FS table

- Configure the /data mount point to the OS FS table by adding the following line

```
/dev/mapper/vg_data-lv_data /data                   ext4     defaults
1 2
```

- Comment out the following line

```
#/dev/mapper/vg_data_old-lv_data /data                   xfs
defaults        0 0
```

- Restart the system

```
reboot
```

- Ensure the /data mount point is mounted using vg_data volume group

```
df -h
output :
Filesystem                         Size  Used Avail Use% Mounted on
/dev/mapper/vg_root-lv_root        4.0G  1.6G  2.5G  39% /
devtmpfs                           7.9G     0  7.9G   0% /dev
tmpfs                              7.9G   56K  7.9G   1% /dev/shm
tmpfs                              7.9G  9.1M  7.9G   1% /run
tmpfs                              7.9G     0  7.9G   0%
/sys/fs/cgroup
/dev/sda1                          2.0G  101M  1.8G   6% /boot
/dev/mapper/vg_data-lv_data        101G   81M   96G   1% /data
/dev/mapper/vg_root-lv_var         4.0G  109M  3.9G   3% /var
/dev/mapper/vg_logs-lv_logs         11G   44M   11G   1% /logs
/dev/mapper/vg_shared-lv_shared    509M   26M  483M   6% /shared
/dev/mapper/vg_root-lv_tmp         2.0G  726M  1.3G  36% /tmp
/dev/mapper/vg_inst-lv_inst        7.0G  2.8G  4.3G  40% /installs
/dev/mapper/vg_app-lv_app          7.0G  1.4G  5.7G  20% /app
/dev/mapper/vg_apptmp-lv_apptmp    4.0G   33M  4.0G   1% /app/tmp
tmpfs                              1.6G     0  1.6G   0% /run/user/0
```

- Start the application services using the Main Admin Menu CLI (option 1 "start all")

Verify The Application Is Working Properly

Login to DPOD's WebUI and use the "Internal Health" screens to verify all components are up and running.

Remove the Old data volume group

- Mark the volume group as non active

```
vgchange -an vg_data_old
output : 0 logical volume(s) in volume group "vg_data_old" now
active
```

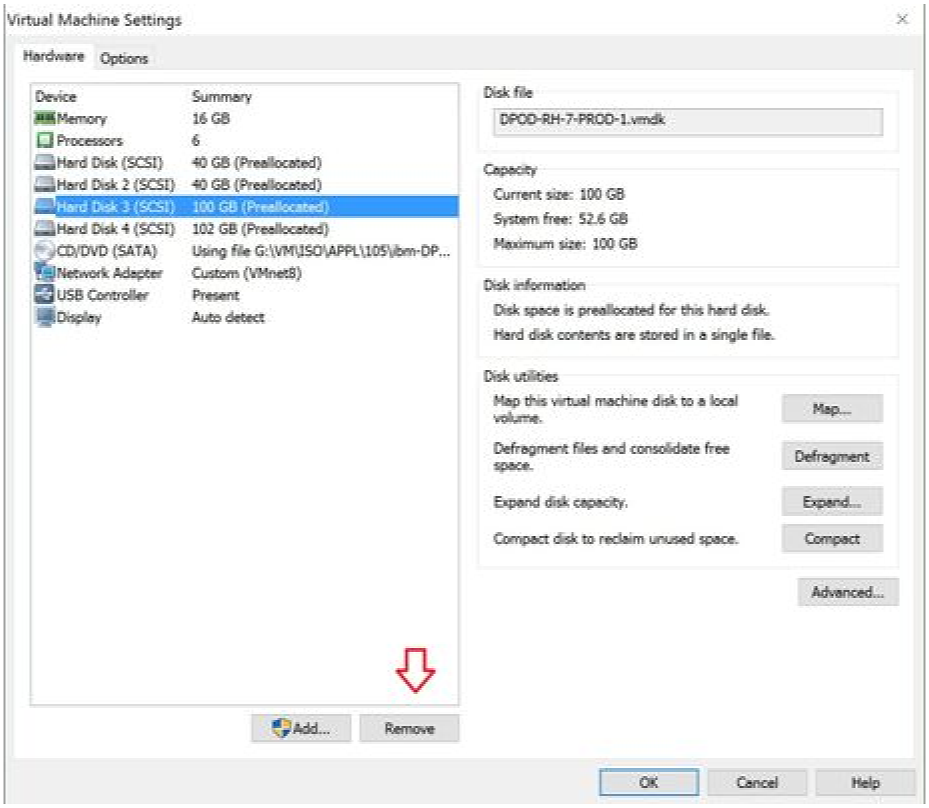
- Export the volume group

```
vgexport vg_data_old
output : Volume group "vg_data_old" successfully exported
```

- Shut down the new system

```
shutdown -h 0
```

- Remove the unused virtual disk from the VM (should be the 3rd virtual hard drive)



Device	Summary
Memory	16 GB
Processors	6
Hard Disk (SCSI)	40 GB (Preallocated)
Hard Disk 2 (SCSI)	40 GB (Preallocated)
Hard Disk 3 (SCSI)	100 GB (Preallocated)
Hard Disk 4 (SCSI)	102 GB (Preallocated)
CD/DVD (SATA)	Using file G:\VM\ISO\APPL\105\ibm-DP...
Network Adapter	Custom (VMnet8)
USB Controller	Present
Display	Auto detect

Disk file

DPOD-RH-7-PROD-1.vmdk

Capacity

Current size: 100 GB

System free: 52.6 GB

Maximum size: 100 GB

Disk information

Disk space is preallocated for this hard disk.

Hard disk contents are stored in a single file.

Disk utilities

Map this virtual machine disk to a local volume.

Defragment files and consolidate free space.

Expand disk capacity.

Compact disk to reclaim unused space.

- Start the VM

Verify The Application Is Working Properly

Login to DPOD's WebUI and use the "Internal Health" screens to verify all components are up and running.

Physical Environment

When using a physical environment the data disk can be either local storage (usually SSD) or a remote central storage (SAN)

In both cases the procedure is similar to the one used for the virtual environment. However, on a physical server the local / remote storage should be physically moved to the new server.

- Edit the New System's OS FS table
- Rename the /data LVM volume Group
- Configure a new disk
- Add the new mount point to the OS FS table
- Verify the application is working properly

Create Staging Directory

Create a staging directory on the new system

```
mkdir -p /installs/system-backup/system-migration
```

Restore Internal DB

Copy the backup directory from the source system to the staging directory.

Invoke the restore command for the internal DB, where :

-t : the restore type (**db**)

-d : the restore source backup directory. In the example below this is /installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56

-f : the source backup file in the backup directory. In the example below this is full-backup-2017-09-13_22-38-56.tar.gz

```
app_restore.sh -t db -d
/installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56
-f full-backup-2017-09-13_22-38-56.tar.gz

stopping application ...
application stopped successfully.
starting restore process ...
restoring internal DB .....
system restore was successful
for more information see log file
/installs/system-backup/db-restore-2017-09-17_15-04-19.log
```

Restore Application Files

Copy the backup directory from the source system to the staging directory (not required if copied during internal DB restore)

Invoke the restore command for the application, where :

-t : the restore type (**app**)

-d : the restore source backup directory. In the example below this is /installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56

-f : the source backup file in the backup directory. In the example below this is full-backup-2017-09-13_22-38-56.tar.gz

```
app_restore.sh -t app -d
/installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56
-f full-backup-2017-09-13_22-38-56.tar.gz

stopping application ...
application stopped successfully.
starting restore process ...
restoring system files ...
making sure files to restore exist in backup file
files to restore exist in backup file
system restore was successful
for more information see log file
/installs/system-backup/app-restore-2017-09-17_15-04-19.log
```

Change the Agent's IP Address

This section is applicable only if the agent's IP address on the new DPOD system is different to the current IP address. In most of the installations the agent's IP address is identical to DPOD's server IP address

If the new DPOD system has a different IP address to the current one, the user must change the "Agent IP" in the nodes management screen :

- Start the application services using the Main Admin Menu CLI (option 1 "start all")
- In the web console navigate to **system nodes** and edit the IP address of the agents in your data node raw.
- Re-configure syslog for the default domain on each monitored device (the Setup Syslog for device on the Device Management section)
- Restart the keepalive service using the Main Admin Menu CLI

Update the Store Configuration File

In order to reconfigure the Store configuration file based on the data disk size follow the section "Update the Store Configuration File" in the "Increase DPOD's Store Space" procedure.

Verify The Application Is Working Properly

Login to DPOD WebUI and use the "Internal Health" screens to verify all components are up and running.

Make sure the new transaction data from the monitored devices is visible using the "Investigate" screen

Post Installation Tasks

Perform the following tasks to activate your product

1. Log in to the Web Console (default username: admin, default password: adminuser)
2. Read and accept the EULA (End User License Agreement)
3. Once logged in, Check system services status (if you didn't setup any monitored devices yet - the Device and Service Resources indicators may be Red)
4. To start monitoring and viewing transnational data you MUST Read the following sections for information on how to perform the required post installation setup commands such as adding a monitored DataPower Gateway .
5. Please complete LDAP configuration steps. The built-in local repository of users, groups and roles is only for POCs and demo usage. To better comply with more strict security requirements it is advised to leave the Local User Registry Management disabled in system parameters (it is disabled by default). When disabled, DPOD will not allow to add or edit any users, roles or groups, and will display a relevant error message.
6. Please consider performing the Optional post installation tasks.

Adding Monitored Devices

Before You Begin

Before adding new monitored devices to DPOD, you may backup the objects that the DPOD will alter during the configuration phase, such as the XML management interface, the WS-M agent etc.
For detailed information regarding IDG DPOD related objects backup and restore see : Backing up and Restoring DPODs IDG related configuration

Before you add a new monitored device to DPOD, ensure to perform the following:

1. Check routing and access from a monitored device:
   The DataPower Gateway needs to route packets to DPOD Agents through the desired interface. Validate through the DataPower's [**control panel->Troubleshooting->TCP Connection Test]**
2. Log-in to DPOD Web Console

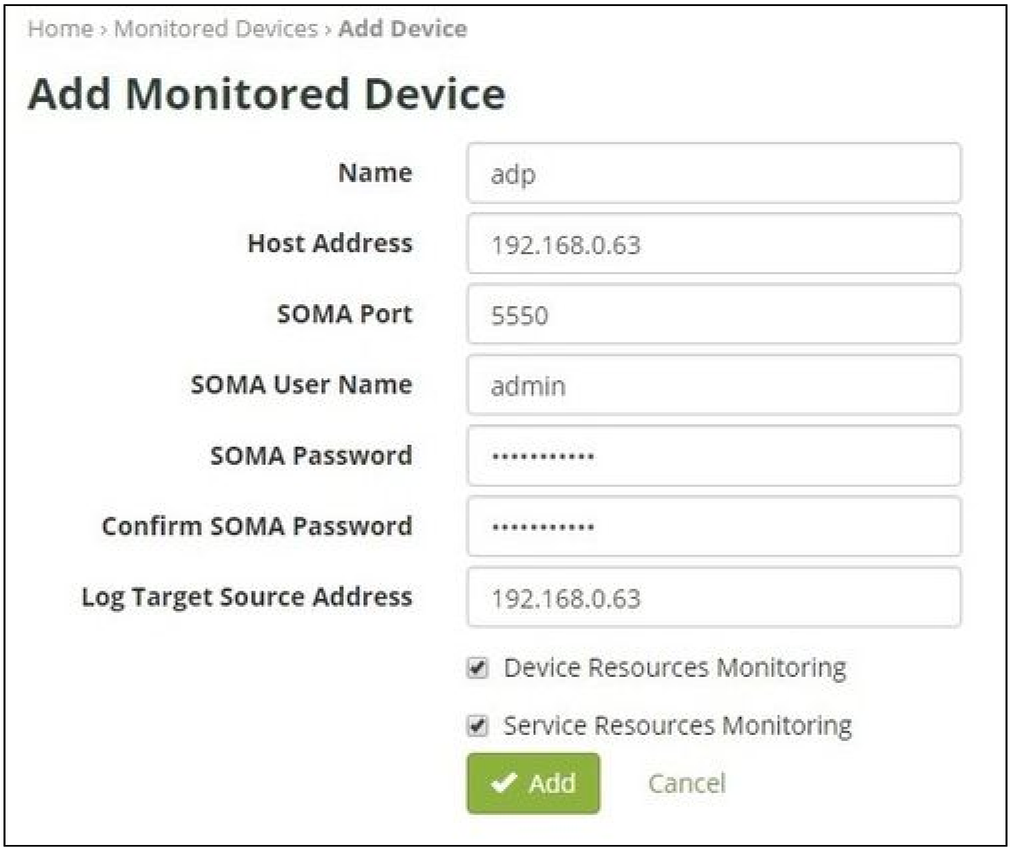
Device Level Configuration

Add The Device In DPOD

> Adding a device with a locale other than EN may cause some DPOD features to not work as expected

1. Inside DPOD's Web Console, navigate to Monitored Devices **[Manage->Devices->Monitored Devices]** and click on “Add Device”
2. Enter the required information. (Consult Device Management for details)
   Note that the device name must be identical to the System Identifier/Appliance Name of the DataPower Gateway as set in the IDG itself, and must meet the requirements detailed in http://www-01.ibm.com/support/docview.wss?uid=swg21668456.

   > If you wish to add a Tenant device, enter the landlord's name but use the tenant's SOMA port, DPOD will display the tenant's name as tenant@landlord



Add Monitored Device

Name: adp

Host Address: 192.168.0.63

SOMA Port: 5550

SOMA User Name: admin

SOMA Password: ••••••••••••

Confirm SOMA Password: ••••••••••••

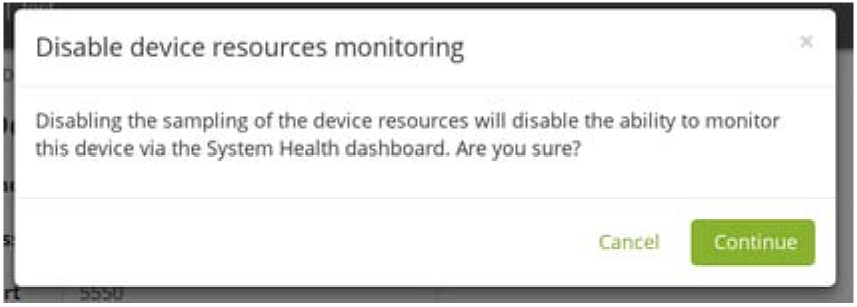
Log Target Source Address: 192.168.0.63

☑ Device Resources Monitoring

☑ Service Resources Monitoring

3. Click “Add”

4. If you choose not to monitor device resources, this message will appear:



Disable device resources monitoring

Disabling the sampling of the device resources will disable the ability to monitor this device via the System Health dashboard. Are you sure?

   This means that this device's health will be missing in System Health dashboard.
   Also, dashboards, reports and alerts based on data collected when monitoring device resources will not work (i.e. Device Resources dashboard).

5. DPOD will add the device. (Verify by locating the new device in the list of monitored devices)

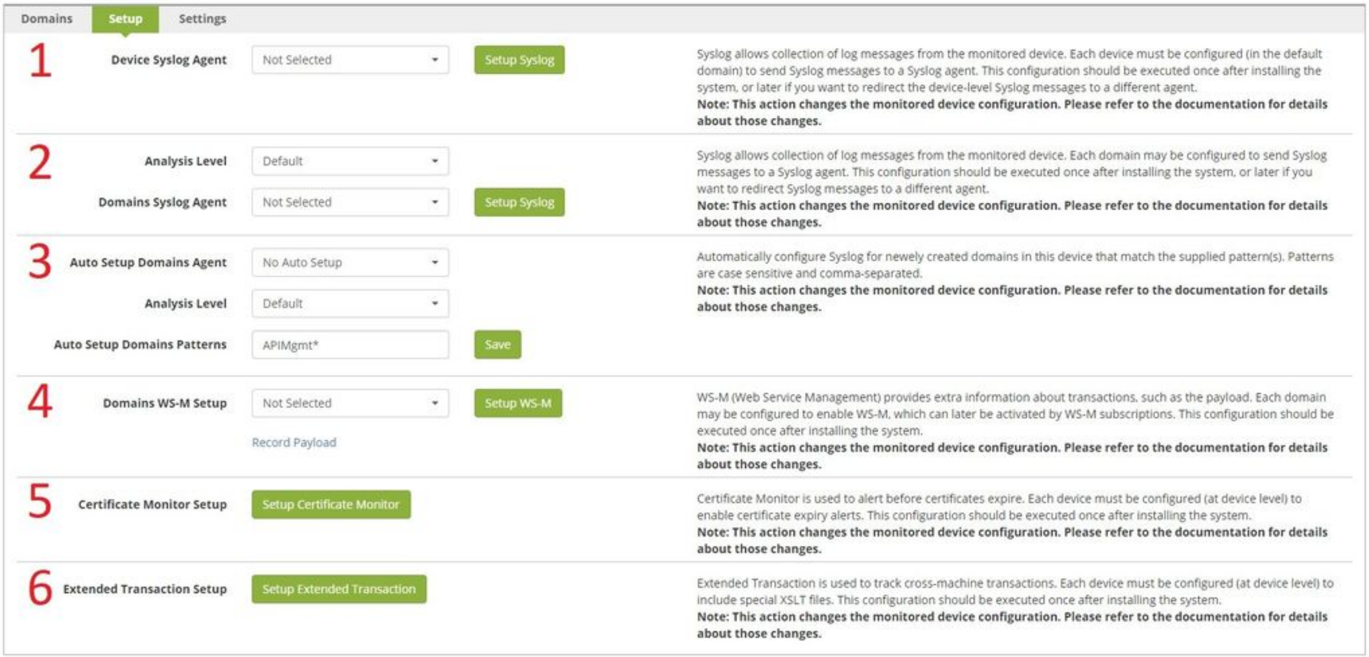
> When updating the "Log Target Source Address" after the device was added and syslog was setup for the device , the user must setup the syslog for device again (see below) in order for the change to take effect on the monitored device (see next item "Setup Syslog For The New Monitored Device").

Configure The New Monitored Device

> If you change DPOD's or the monitored device's IP address, you will need to repeat the setup

> If you wish to monitor transactions in the default domain, please follow the instructions in Monitoring Transactions in the Default Domain

Right after adding the device, the "Setup" tab will be displayed, the tab is divided into six parts.



1 Device Syslog Agent: Not Selected [Setup Syslog]

Syslog allows collection of log messages from the monitored device. Each device must be configured (in the default domain) to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect the device-level Syslog messages to a different agent.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

2 Analysis Level: Default

Domains Syslog Agent: Not Selected [Setup Syslog]

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect Syslog messages to a different agent.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

3 Auto Setup Domains Agent: No Auto Setup

Analysis Level: Default

Auto Setup Domains Patterns: APIMgmt* [Save]

Automatically configure Syslog for newely created domains in this device that match the supplied pattern(s). Patterns are case sensitive and comma-separated.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

4 Domains WS-M Setup: Not Selected [Setup WS-M]

Record Payload

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration should be executed once after installing the system.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

5 Certificate Monitor Setup: [Setup Certificate Monitor]

Certificate Monitor is used to alert before certificates expire. Each device must be configured (at device level) to enable certificate expiry alerts. This configuration should be executed once after installing the system.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

6 Extended Transaction Setup: [Setup Extended Transaction]

Extended Transaction is used to track cross-machine transactions. Each device must be configured (at device level) to include special XSLT files. This configuration should be executed once after installing the system.
Note: This action changes the monitored device configuration. Please refer to the documentation for details about those changes.

1. **Device Syslog Agent -** select the desired Syslog Agent according to the architecture design, click "Setup Syslog" and wait until the action completes successfully.

2. **Setup Syslog for All Domains** -

   > This section will apply the same setup too all domains in the device, to select a different configuration for each domain, see the section "Domain Level Configuration" later on this page.

Select the desired Analysis Level, select the Syslog agent according to the architecture design and click "Setup Syslog", the operation may take a few minutes

3. **Auto Setup Domains (Optional)** -
This feature will automatically detect and setup new domains created on the monitored device. This is especially useful for dynamically created API Connect domains.
Select a Syslog agent that the domains should report to, select the desired Analysis Level, enter the domain pattern (you may use asterisk as wildcard) and click save.
DPOD will scan the monitored devices every 2 minutes and will setup the new domain. You may change the scan interval on the system parameters page. (A UI service restart via the CLI is required after changing this interval)
For domains that match the auto setup pattern - DPOD will also try to detect if any domain was reset and setup it again.

4. **Domains WS-M Setup (Optional)**

> This section will apply the same setup too all domains in the device, to select a different configuration for each domain, see the section "Domain Level Configuration" later on this page.

If you wish to record and view payloads, or to record API-C policy variables, select the desired WS-M Agent according to the architecture design and click "Setup WS-M", the operation may take a few minutes.
For supported WS-M payload capture services see IDG WS-M payload capture support.
Click on "Record Payload" to open the payload capture page where you can start capturing payloads

5. **Certificate Monitor Setup (Optional)**
If you wish to use DPOD's expired certificate dashboard, click on "Setup Certificate Monitor"
Consult the System Parameters List ("Certificate monitoring duration in days") for information regarding the time interval parameter.

6. **Extended Transaction Setup (Optional, Deprecated)**

> **This feature is deprecated and was replaced by a non-intrusive method.**

Please **do not** use the button unless advised by L2/L3 support.

Domain Level Configuration (Optional)

if your architectural design dictates a different configuration for domains on the same machine, you can configure them separately:

1. Navigate to the domain setup page [Manage Devices Monitored Devices]
2. Click the device name
3. Click the domain name
4. Click "Setup"

> Domains may be redirected to different Syslog agents according to the architecture design. Additionally, you may choose to enable WS-M on specific domains only etc. If this is required, follow the steps below to configure specific domains. Otherwise you may skip this section

Syslog setup (Optional)

Under "Syslog Setup", select the desired Analysis Level, select the desired Syslog Agent according to the architecture design, click "Setup Syslog" and wait until the action completes successfully.

Domain WS-M setup (Optional)

Select the desired WS-M Agent according to the architecture design. Click "Setup WS-M" and wait until the action completes successfully.
For supported WS-M payload capture services see IDG WS-M payload capture support.
Click on "Record Payload" to open the payload capture page where you can start capturing payloads

Extended Transaction setup for all services (Optional, Deprecated)

Please **do not** use the button unless advised by L2/L3 support, this feature was deprecated and was replaced by a non-intrusive method.

Under "Services Extended Transaction Setup", click "Setup Extended Transaction for all services" and wait until the action completes successfully.

> This step will **MODIFY SERVICES PROCESSING POLICY**. You must test and verify that the services are not affected by this change

before setting this up on production environments.

MONITORING TENANT DEVICES

DPOD supports monitoring of Tenant devices (introduced in IDG 7.6).
Add the tenant device to DPOD in the same way you add any other device, enter the landlord's name as the device name, and in the SOMA port enter the tenant's SOMA port.
DPOD will handle the tenant device the same as any other device, and will display the tenant as tenant@landlord (for example, apicTenant@device1)

The following features are currently not supported for Tenant devices:

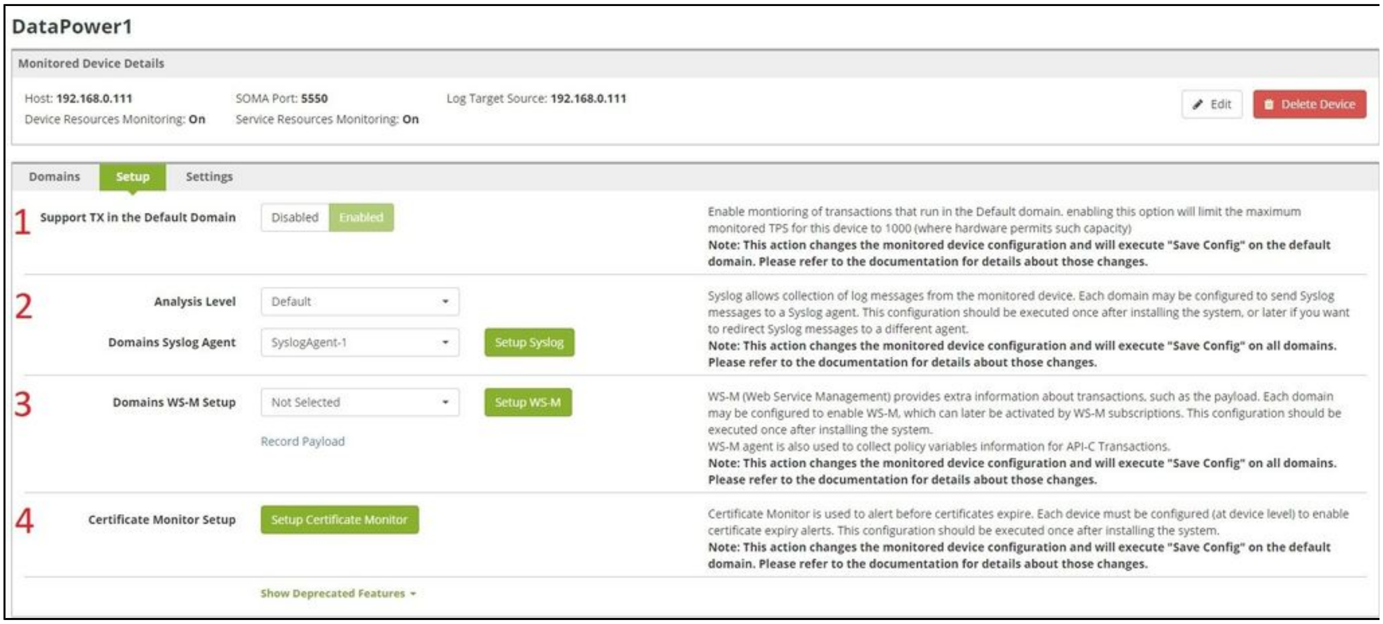
- Device resource monitoring
- Appliance Maintenance (Backup, Sync, Firmware Upgrade)
- Extended Transaction

MONITORING TRANSACTIONS IN THE DEFAULT DOMAIN

> Monitoring transactions in the default domain will limit the maximum monitored TPS for the device to 1000 (where hardware permits such capacity)

To Enable monitoring transactions in the default domain, change the value of the system parameter "Allow Monitoring Transactions in Default Domain" to "true" and refresh the page.

Go to the Monitored Devices page and select the device you want to monitor.



DataPower1

Monitored Device Details

Host: **192.168.0.111** SOMA Port: **5550** Log Target Source: **192.168.0.111**
Device Resources Monitoring: **On** Service Resources Monitoring: **On**

Support TX in the Default Domain: Enabled

Enable montioring of transactions that run in the Default domain. enabling this option will limit the maximum monitored TPS for this device to 1000 (where hardware permits such capacity)
Note: This action changes the monitored device configuration and will execute "Save Config" on the default domain. Please refer to the documentation for details about those changes.

Analysis Level: Default

Domains Syslog Agent: SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect Syslog messages to a different agent.
Note: This action changes the monitored device configuration and will execute "Save Config" on all domains. Please refer to the documentation for details about those changes.

Domains WS-M Setup: Not Selected

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration should be executed once after installing the system.
WS-M agent is also used to collect policy variables information for API-C Transactions.
Note: This action changes the monitored device configuration and will execute "Save Config" on all domains. Please refer to the documentation for details about those changes.

Certificate Monitor Setup

Certificate Monitor is used to alert before certificates expire. Each device must be configured (at device level) to enable certificate expiry alerts. This configuration should be executed once after installing the system.
Note: This action changes the monitored device configuration and will execute "Save Config" on the default domain. Please refer to the documentation for details about those changes.

1. **Support TX in the Default Domain**
   When the option is disabled - the rest of the screen will look like, and behave as described in the add monitored devices page, transactions in the default domain will not be monitored.
   When the option is enabled - the screen will behave as described below.
   The operation may take a few minutes.

   > Changing this option will immediately remove all of DPOD's log targets from the monitored device.
   > If the device was already monitored - you will need to setup syslogs for all domains again, just changing this option is not enough.

2. **Setup Syslog for All Domains -** Select the desired Analysis Level, select the Syslog agent and click "Setup Syslog", the operation may take a few minutes

   > Monitoring transactions in the default domain will cause all domains in the monitored device to report to the same DPOD syslog agent, it is not possible to choose a different syslog agent per domain.

   > The "Auto Setup Domains" option is redundant and is not available when monitoring transactions in the default domain - all new domains will be monitored automatically..

3. **Domains WS-M Setup (Optional) -** If you wish to record and view payloads, or to record API-C policy variables, select the desired WS-M Agent according to the architecture design and click "Setup WS-M", the operation may take a few minutes.
   For supported WS-M payload capture services see IDG WS-M payload capture support.
   Click on "Record Payload" to open the payload capture page where you can start capturing payloads
4. **Certificate Monitor Setup (Optional)**
   If you wish to use DPOD's expired certificate dashboard, click on "Setup Certificate Monitor"
   Consult the System Parameters List ("Certificate monitoring duration in days") for information regarding the time interval parameter.

Optional configuration tasks

1. Send reports, alerts, internal alerts or maintenance events via Email: Setup the SMTP host, password, port and user name in the system parameters page
2. Send reports via Email: configure the reports Email destination
3. Publish alerts via syslog: configure the alerts syslog server hostname and port in the system parameters page
4. Setup DevOps portal if you want to use DevOps features such as Remote or Local WSDL validation and promotion.
5. Receive internal DPOD health checks alerts via syslog or Email: enter the Email recipients and change the value for "Internal Alerts - Send Email on Alert" , "Internal Alerts - Email Destination Address for Alerts" and "Internal Alerts - Send Syslog on Alert" in the system parameters page. Restart the keepalive service via app-util.sh after changing these parameters
6. Publish DPOD maintenance events (backup, sync, firmware upgrade) via syslog: configure the maintenance syslog server hostname and port in the system parameters page
7. Use the backup appliance feature: change the "Backups - Destination Path" in the system parameters page to a new **dedicated** mount point
8. Use the appliance firmware upgrade feature:
   a. Change the "Firmware Upgrade - Repository Path" in the system parameters page to a new **dedicated** mount point.
   b. The system parameter "Firmware Upgrade - Local Node IP Address" contains the address which monitored devices should access DPOD via SSH

   > make sure the address is correct and each monitored device can access this address via ssh (port 22)

   c. The system parameters "Firmware Upgrade - OS User Name" and "Firmware Upgrade - OS User Password" contain the user and password that will be used to access DPOD via SSH,

   For Appliance Installation - The user is initially locked, you will need to unlock the user, change its password and update the system parameter.

   i. Login to DPOD as root user
   ii. Unlock the user by issuing the command: "passwd -u productuser1"
   iii. Change the user's password by issuing: "passwd productuser1", the maximum password length is 30 characters.
   iv. Update DPOD's system parameter ("Firmware Upgrade - OS User Password") with the new password

   For Non Appliance installation or Docker container installation - system administrator should create a user called "productuser1", and update DPOD's system parameter ("Firmware Upgrade - OS User Password") with its password
   example : OS command for creating the OS user :

   ```
   useradd -md /home/productuser1 -s /bin/bash  productuser1
   ```

9. Receive Syslog notification for the backup, sync or firmware upgrade features: change "Maintenance Syslog Notifications Destination Hostname" in the system parameters page
10. Security hardening such as: replace self signed certificate of the web console and limit admin dashboard to specific IP addresses.
11. Externalize the console to support users with no access to the DPOD regulate network.

CONFIGURING NOTIFICATIONS BY EMAIL/WS/SYSLOG/LOCAL FILE

Notifications are sent by reports/alerts/share and maintenance plans

Configure Notifications by Email

To enable DPOD to send notifications via email, you will first need to configure SMTP in the system.

1. Obtain the SMTP details for your email server
2. Login to the Web Console
3. Navigate to **[Manage->System->System Parameters]**
4. Enter the correct values for the **Email** and **Email SMTP** categories according to your organization's SMTP configuration.
5. Enable/Disable **Email SMTP** by entering the correct values for the **Alerts** and **Reports** categories.
6. For more information see system parameters.

Configure Notifications by WS

To enable DPOD to send reports via WS, you will first need to configure SMTP in the system.

1. Obtain the SMTP details for your email server
2. Login to the Web Console
3. Navigate to **[Manage->System->System Parameters]**
4. Enter the correct values for the **Email** and **Email SMTP WS** categories according to your organization's SMTP configuration.
5. Enable/Disable **Email SMTP WS** by entering the correct values for the **Alerts** and **Reports** categories.
6. For more information see system parameters.

Configure Notifications by Syslog

1. Login to the Web Console
2. Navigate to **[Manage->System->System Parameters]**
3. Enter the correct values for the **Maintenance** and **Alerts** categories according to your organization's configuration.
4. For more information see system parameters.

Configure Notifications by Publishing to Local File

1. Login to the Web Console
2. Navigate to **[Manage->System->System Parameters]**
3. Enable/Disable publishing to local file by entering the correct values for the **Alerts** and **Reports** categories.
4. For more information see system parameters.

SETUP A CELL ENVIRONMENT

Overview

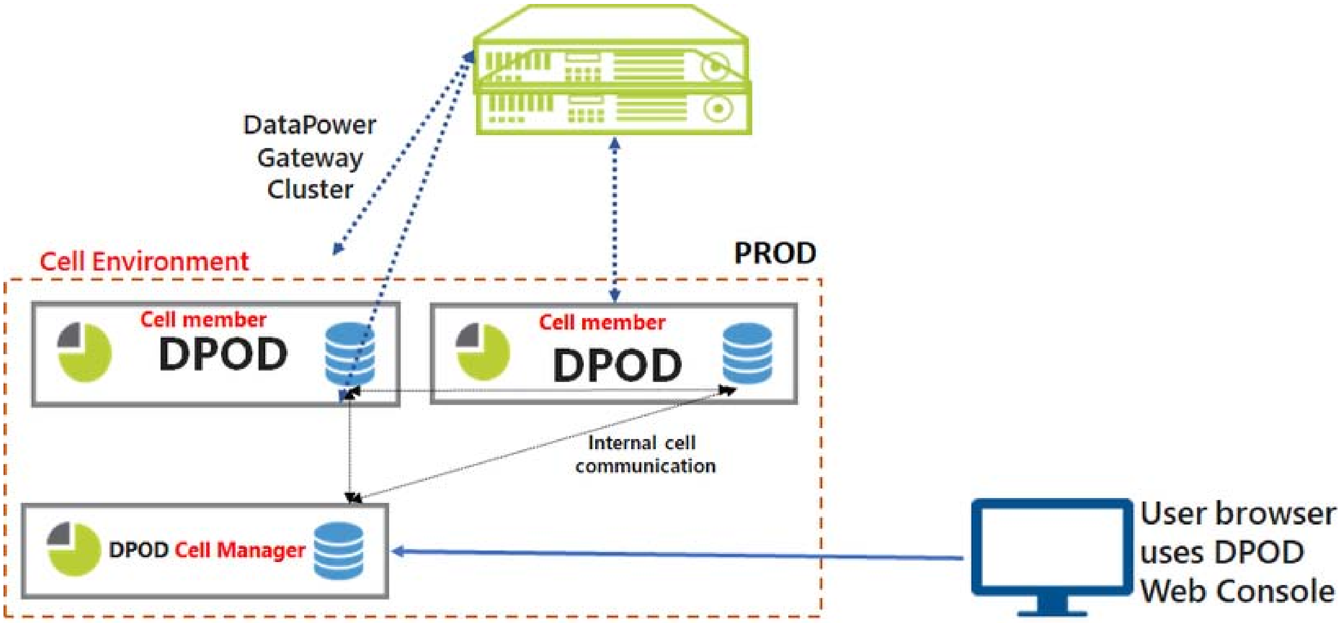
Federated architecture best fits customers that execute high load (thousands of transactions per seconds) in their gateways, where the vast majority of the transactions is executed on-premise.

The cell environment implements the federated architecture by distributing DPOD's Store and DPOD's processing (using DPOD's agents) across different federated servers.

The cell environment has two main components:

- Cell Manager - a DPOD server (virtual or physical) that manages all Federated Cell Members (FCMs) as well as providing central DPOD services such as Web Console, reports, alerts, etc.
- Federated Cell Member (FCM) - a DPOD server (usually physical with local high speed storage) that includes Store data nodes and agents (Syslog and WS-M) for collecting, parsing and storing data. There could be one or more federated cell members per cell.

The following diagram describes the Cell Environment:


DataPower Gateway Cluster
Cell Environment
PROD
Cell member
DPOD
Cell member
DPOD
Internal cell communication
DPOD Cell Manager
User browser uses DPOD Web Console

The following procedure describes the process of establishing a DPOD cell environment.

Prerequisites

1. DPOD cell manager and federated cell members **must be** with the same version (minimum version is v1.0.8.5).
2. DPOD cell manager can be installed in both **Appliance Mode** or **Non-Appliance Mode** with **Medium Load** architecture type, as detailed in the Hardware and Software Requirements. The manager server can be both virtual or physical.
3. DPOD federated cell member (FCM) should be installed in **Non-appliance Mode** with **High_20dv** architecture type, as detailed in the Hardware and Software Requirements.
4. Each cell component (manager / FCM) should have two network interfaces:
   a. External interface - for DPOD users to access the Web Console and for communication between DPOD and Monitored Gateways.
   b. Internal interface - for internal DPOD components inter-communication (should be a 10Gb Ethernet interface).
5. Network ports should be opened in the network firewall as detailed below:

From	To	Ports (Defaults)	Protocol	Usage
DPOD Cell Manager	Each Monitored Device	5550 (TCP)	HTTP/S	Monitored device administration management interface
DPOD Cell Manager	DNS Server	TCP and UDP 53	DNS	DNS services. Static IP address may be used.
DPOD Cell Manager	NTP Server	123 (UDP)	NTP	Time synchronization
DPOD Cell Manager	Organizational mail server	25 (TCP)	SMTP	Send reports by email

DPOD Cell Manager	LDAP	TCP 389 / 636 (SSL). TCP 3268 / 3269 (SSL)	LDAP	Authentication & authorization. Can be over SSL.
DPOD Cell Manager	Each DPOD Federated Cell Member	443 (TCP)	HTTP/S	Communication (data + management)
DPOD Cell Manager	Each DPOD Federated Cell Member	9300-9305 (TCP)	ElasticSearch	ElasticSearch Communication (data + management)
NTP Server	DPOD Cell Manager	123 (UDP)	NTP	Time synchronization
Each Monitored Device	DPOD Cell Manager	60000-60003 (TCP)	TCP	SYSLOG Data
Each Monitored Device	DPOD Cell Manager	60020-60023 (TCP)	HTTP/S	WS-M Payloads
Users IPs	DPOD Cell Manager	443 (TCP)	HTTP/S	DPOD's Web Console
Admins IPs	DPOD Cell Manager	22 (TCP)	TCP	SSH
Each DPOD Federated Cell Member	DPOD Cell Manager	443 (TCP)	HTTP/S	Communication (data + management)
Each DPOD Federated Cell Member	DPOD Cell Manager	9200, 9300-9400	ElasticSearch	ElasticSearch Communication (data + management)
Each DPOD Federated Cell Member	DNS Server	TCP and UDP 53	DNS	DNS services
Each DPOD Federated Cell Member	NTP Server	123 (UDP)	NTP	Time synchronization
NTP Server	Each DPOD Federated Cell Member	123 (UDP)	NTP	Time synchronization
Each Monitored Device	Each DPOD Federated Cell Member	60000-60003 (TCP)	TCP	SYSLOG Data
Each Monitored Device	Each DPOD Federated Cell Member	60020-60023 (TCP)	HTTP/S	WS-M Payloads
Admins IPs	Each DPOD Federated Cell Member	22 (TCP)	TCP	SSH

Cell Manager Installation

Prerequisites

- DPOD cell manager should be installed in **Non-Appliance Mode** with **Medium Load** architecture type, as detailed in the Hardware and Software Requirements. The manager server can be both virtual or physical.
- Install the following software package (RPM): **bc**

Installation

Install DPOD as described in one of the following installation procedures:

> **Important** !! During the Cell Manager installation the user will be asked to choose the data disk type (SSD / non SSD) - choose the cell members disk type (should be SSD)

- Non-appliance Mode: Installation procedure

> As described in the prerequisites section, the cell manager should have two network interfaces.
>
> When installing DPOD, the user is prompted to choose the IP address for the Web Console - this should be the IP address of the external network interface.

- After DPOD installation is complete, the user should execute the following operating system performance optimization script:

```
/app/scripts/tune-os-parameters.sh
```

Federated Cell Member Installation

The following section describes the installation process of a single Federated Cell Member (FCM). User should repeat the procedure for every FCM installation.

Prerequisites

- DPOD federated cell member (FCM) should be installed in **Non-appliance Mode** with **High_20dv** architecture type, as detailed in the Hardware and Software Requirements.
- Install the following software package (RPM): **bc**
- The following software packages (RPMs) are recommended for system maintenance and troubleshooting, but are not required: **telnet client, net-tools, iftop, tcpdump, pciutils**

Installation

DPOD Installation

- Install DPOD in **Non-Appliance Mode:** Installation procedure
- The four letter Installation Environment Name should be identical to the one that was chosen for the Cell Manager.

As described in the prerequisites section, the federated cell member should have two network interfaces.

When installing DPOD, the user is prompted to choose the IP address for the Web Console - this should be the IP address of the external network interface (although the FCM does not run the Web Console service).

- After DPOD installation is complete, the user should execute the following operating system performance optimization script:

```
/app/scripts/tune-os-parameters.sh
```

User should reboot the server for the new performance optimization to take effect.

Preparing Cell Member for Federation

Preparing Mount Points

The cell member is usually a "bare metal" server with NVMe disks for maximizing server throughput.

Each of the Store's logical node (service) will be bound to a specific physical processor, disks and memory using NUMA (Non-Uniform Memory Access) technology.

The default cell member configuration assumes 6 NVMe disks which will serve 3 Store logical nodes (2 disks per node).

The following OS mount points should be configured by the user before federating the DPOD cell member to the cell environment.

We highly recommend the use of LVM (Logical Volume Manager) to allow flexible storage for future storage needs.

Empty cells in the following table should be completed by the user, based on their specific hardware:

Store Node	Mount Point Path	Disk Bay	PCI Slot Number	Disk Serial	Disk OS Path	NUMA node (CPU #)
2	/data2					
2	/data22					
3	/data3					
3	/data33					
4	/data4					
4	/data44					

How to Identify Disk OS Path and Disk Serial

1. To identify which of the server's NVMe disk bays is bound to which of the CPUs, use the hardware manufacture documentation. Also, write down the disk's serial number by visually observing the disk.
2. In order to identify the disk **OS path** (e.g.: /dev/nvme01n), disk **serial** and disk **NUMA node** use the following command :
   a. Identify all NVMe Disks installed on the server

```
lspci -nn | grep NVM

expected output :

5d:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
5e:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
ad:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
ae:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
c5:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
c6:00.0 Non-Volatile memory controller [0108]: Intel
Corporation Express Flash NVMe P4500 [8086:0a54]
```

   b. Locate disk's NUMA node
   Use the disk PCI slot listed in previous command to identify the NUMA node (the first disk PCI slot is : **5d:00.0**)

```
lspci  -s 5d:00.0 -v

expected output :

5d:00.0 Non-Volatile memory controller: Intel Corporation
Express Flash NVMe P4500 (prog-if 02 [NVM Express])
        Subsystem: Lenovo Device 4712
        Physical Slot: 70
        Flags: bus master, fast devsel, latency 0, IRQ 93, NUMA
node 1
        Memory at e1310000 (64-bit, non-prefetchable)
[size=16K]
        Expansion ROM at e1300000 [disabled] [size=64K]
        Capabilities: [40] Power Management version 3
        Capabilities: [50] MSI-X: Enable+ Count=129 Masked-
        Capabilities: [60] Express Endpoint, MSI 00
        Capabilities: [a0] MSI: Enable- Count=1/1 Maskable-
64bit+
        Capabilities: [100] Advanced Error Reporting
        Capabilities: [150] Virtual Channel
        Capabilities: [180] Power Budgeting <?>
        Capabilities: [190] Alternative Routing-ID
Interpretation (ARI)
        Capabilities: [270] Device Serial Number
55-cd-2e-41-4f-89-0f-43
        Capabilities: [2a0] #19
        Capabilities: [2d0] Latency Tolerance Reporting
        Capabilities: [310] L1 PM Substates
        Kernel driver in use: nvme
        Kernel modules: nvme
```

From the command output (line number 8) we can identify the NUMA node (Flags: bus master, fast devsel, latency 0, IRQ 93, **NUMA node 1**)

c. Identify NVMe Disks path
Use the disk PCI slot listed in previous command to identify the disk's block device path

```
ls -la /sys/dev/block |grep  5d:00.0

expected output :
lrwxrwxrwx. 1 root root 0 Nov  5 08:06 259:4 ->
../../devices/pci0000:58/0000:58:00.0/0000:59:00.0/0000:5a:02.0
/0000:5d:00.0/nvme/nvme0/nvme0n1
```

Use the last part of the device path (**nvme0n1**) as input for the following command :

```
nvme -list |grep nvme0n1

expected output :

/dev/nvme0n1     PHLE822101AN3P2EGN   SSDPE2KE032T7L
1           3.20  TB /   3.20  TB    512   B +  0 B   QDV1LV45
```

The disk's path is **/dev/nvme0n1**

1. Use the disk bay number and the disk serial number (visually identified) and correlate them with the output of the disk tool to identify the disk OS path.

Example for Mount Points and Disk Configurations

Store Node	Mount Point Path	Disk Bay	PCI Slot Number	Disk Serial	Disk OS Path	NUMA node (CPU #)
2	/data2	1	2	PHLE822101AN3PXXXX	/dev/nvme0n1	1
2	/data22	2			/dev/nvme1n1	1
3	/data3	4			/dev/nvme2n1	2
3	/data33	5			/dev/nvme3n1	2
4	/data4	12			/dev/nvme4n1	3
4	/data44	13			/dev/nvme5n1	3

Example for LVM Configuration

```
pvcreate -ff /dev/nvme0n1
vgcreate vg_data2 /dev/nvme0n1
lvcreate -l 100%FREE -n lv_data vg_data2
mkfs.xfs -f /dev/vg_data2/lv_data

pvcreate -ff /dev/nvme1n1
vgcreate vg_data22 /dev/nvme1n1
lvcreate -l 100%FREE -n lv_data vg_data22
mkfs.xfs /dev/vg_data22/lv_data
```

/etc/fstab file:

```
/dev/vg_data2/lv_data    /data2                   xfs     defaults
0 0
/dev/vg_data22/lv_data   /data22                   xfs     defaults
0 0
/dev/vg_data3/lv_data    /data3                   xfs     defaults
0 0
/dev/vg_data33/lv_data   /data33                   xfs     defaults
0 0
/dev/vg_data4/lv_data    /data4                   xfs     defaults
0 0
/dev/vg_data44/lv_data   /data44                   xfs     defaults
0 0
```

Create directories for the new data mount points

```
mkdir -p /data2 /data22 /data3 /data33 /data4 /data44
```

Example for the Final Configuration for 3 Store's nodes

This example does not include other mount points needed, as describe in Hardware and Software Requirements.

```
# lsblk

NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
nvme0n1             259:0    0   2.9T  0 disk
vg_data2-lv_data  253:6    0   2.9T  0 lvm  /data2
nvme1n1             259:5    0   2.9T  0 disk
vg_data22-lv_data 253:3    0   2.9T  0 lvm  /data22
nvme2n1             259:1    0   2.9T  0 disk
vg_data3-lv_data  253:2    0   2.9T  0 lvm  /data3
nvme3n1             259:2    0   2.9T  0 disk
vg_data33-lv_data 253:5    0   2.9T  0 lvm  /data33
nvme4n1             259:4    0   2.9T  0 disk
vg_data44-lv_data 253:7    0   2.9T  0 lvm  /data44
nvme5n1             259:3    0   2.9T  0 disk
vg_data4-lv_data  253:8    0   2.9T  0 lvm  /data4
```

Install NUMA Software

```
yum install numactl
```

Preparing Local OS Based Firewall

Most Linux-based OS uses a local firewall service (e.g.: iptables / firewalld).

Since the OS of the Non-Appliance Mode DPOD installation is provided by the user, it is under the user's responsibility to allow needed connectivity to and from the server.

User should make sure needed connectivity detailed in Network Ports Table is allowed on the OS local firewall service.

> When using DPOD Appliance mode installation for the cell manager, local OS based firewall service is handled by the cell member federation script.

Cell Member Federation

In order to federate and configure the cell member, run the following script in the **cell manager** once per cell member.

For instance, to federate two cell members, the script should be run twice (in the cell manager) - first time with the IP address of the first cell member, and second time with the IP address of the second cell member.

Important: The script should be executed using the OS **root** user.

```
/app/scripts/configure_cell_manager.sh -a <internal IP address of the
cell member> -g <external IP address of the cell member>
For example: /app/scripts/configure_cell_manager.sh -a 172.18.100.34 -g
172.17.100.33
```

Example for a Successful Execution

```
/app/scripts/configure_cell_manager.sh -a 172.18.100.36 -g 172.17.100.35

2018-10-22_16-13-16 INFO Cell Configuration
2018-10-22_16-13-16 INFO ===============================
2018-10-22_16-13-18 INFO
2018-10-22_16-13-18 INFO Log file is :
/installs/logs/cell_manager_configuration-2018-10-22_16-13-16.log
2018-10-22_16-13-18 INFO
2018-10-22_16-13-18 INFO Adding new cell member with the following
configuration :
2018-10-22_16-13-18 INFO Cell member internal address 172.18.100.36
2018-10-22_16-13-18 INFO Cell member external address 172.17.100.35
2018-10-22_16-13-18 INFO Syslog agents using TCP ports starting with
60000
2018-10-22_16-13-18 INFO Wsm agents using TCP ports starting with 60020
2018-10-22_16-13-18 INFO
2018-10-22_16-13-18 INFO During the configuration process the system
will be shut down, which means that new data will not be collected and
the Web Console will be unavailable for users.
2018-10-22_16-13-18 INFO Please make sure the required network
connectivity (e.g. firewall rules) is available between all cell
components (manager and members) according to the documentation.
2018-10-22_16-13-18 INFO
2018-10-22_16-13-20 INFO Please choose the IP address for the cell
manager server internal address followed by [ENTER]:
2018-10-22_16-13-20 INFO 1.) 172.18.100.32
2018-10-22_16-13-20 INFO 2.) 172.17.100.31
1
2018-10-22_16-14-30 INFO Stopping application ...
2018-10-22_16-15-16 INFO Application stopped successfully.
root@172.18.100.36's password:
2018-10-22_16-21-41 INFO Cell member configuration ended successfully.
2018-10-22_16-21-45 INFO Stopping application ...
2018-10-22_16-22-31 INFO Application stopped successfully.
2018-10-22_16-22-31 INFO Starting application ...
```

Note that the script writes two log file, one in the cell manager and one in the cell member. The log file names are mentioned in the script's output.
Example for a Failed Execution

```
/app/scripts/configure_cell_manager.sh -a 172.18.100.36 -g 172.17.100.35

2018-10-22_16-05-03 INFO Cell Configuration
2018-10-22_16-05-03 INFO ===============================
2018-10-22_16-05-05 INFO
2018-10-22_16-05-05 INFO Log file is :
/installs/logs/cell_manager_configuration-2018-10-22_16-05-03.log
2018-10-22_16-05-05 INFO
2018-10-22_16-05-05 INFO Adding new cell member with the following
configuration :
2018-10-22_16-05-05 INFO Cell member internal address 172.18.100.36
2018-10-22_16-05-05 INFO Cell member external address 172.17.100.35
2018-10-22_16-05-05 INFO Syslog agents using TCP ports starting with
60000
2018-10-22_16-05-05 INFO Wsm agents using TCP ports starting with 60020
2018-10-22_16-05-05 INFO
2018-10-22_16-05-05 INFO During the configuration process the system
will be shut down, which means that new data will not be collected and
the Web Console will be unavailable for users.
2018-10-22_16-05-05 INFO Please make sure the required network
connectivity (e.g. firewall rules) is available between all cell
components (manager and members) according to the documentation.
2018-10-22_16-05-05 INFO
2018-10-22_16-05-06 INFO Please choose the IP address for the cell
manager server internal address followed by [ENTER]:
2018-10-22_16-05-06 INFO 1.) 172.18.100.32
2018-10-22_16-05-06 INFO 2.) 172.17.100.31
1
2018-10-22_16-05-09 INFO Stopping application ...
2018-10-22_16-05-58 INFO Application stopped successfully.
root@172.18.100.36's password:
2018-10-22_16-06-46 ERROR Starting rollback
2018-10-22_16-06-49 WARN Issues found that may need attention !!
2018-10-22_16-06-49 INFO Stopping application ...
2018-10-22_16-07-36 INFO Application stopped successfully.
2018-10-22_16-07-36 INFO Starting application ...
```

In case of a failure, the script will try to rollback the configuration changes it made, so the problem can be fixed before rerunning it again.

Cell Member Federation Post Steps

NUMA configuration

DPOD cell member is using NUMA (Non-Uniform Memory Access) technology. The default cell member configuration binds DPOD's agent to CPU 0 and the Store's nodes to CPU 1.
If the server has 4 CPUs, the user should edit the service files of nodes 2 and 3 and change the bind CPU to 2 and 3 respectively.
Identifying NUMA Configuration

To identify the amount of CPUs installed on the server, use the NUMA utility:

```
numactl -s

Example output for 4 CPU server :

policy: default
preferred node: current
physcpubind: 0 1 2 3 4 5 6 7 8 9 10 11 12
cpubind: 0 1 2 3
nodebind: 0 1 2 3
membind: 0 1 2 3
```

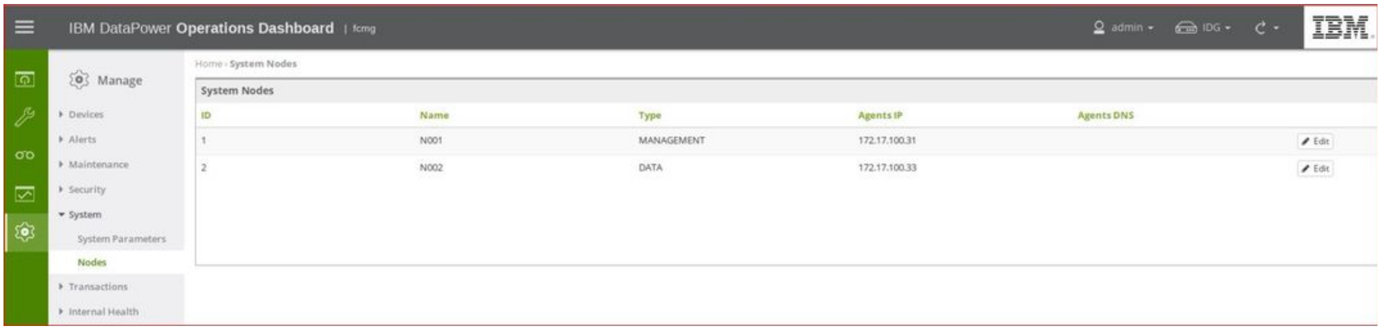
Alter Store's Node 2 and 3 (OPTIONAL - only if the server has 4 CPUs)

The services files are located on the directory /etc/init.d/ with the name MonTier-es-raw-trans-Node-2 and MonTier-es-raw-trans-Node-3.

```
For node MonTier-es-raw-trans-Node-2
OLD VALUE : numa="/usr/bin/numactl --membind=1 --cpunodebind=1"
NEW VALUE : numa="/usr/bin/numactl --membind=2 --cpunodebind=2"

For node MonTier-es-raw-trans-Node-3
OLD VALUE : numa="/usr/bin/numactl --membind=1 --cpunodebind=1"
NEW VALUE : numa="/usr/bin/numactl --membind=3 --cpunodebind=3"
```

Cell Member Federation Verification

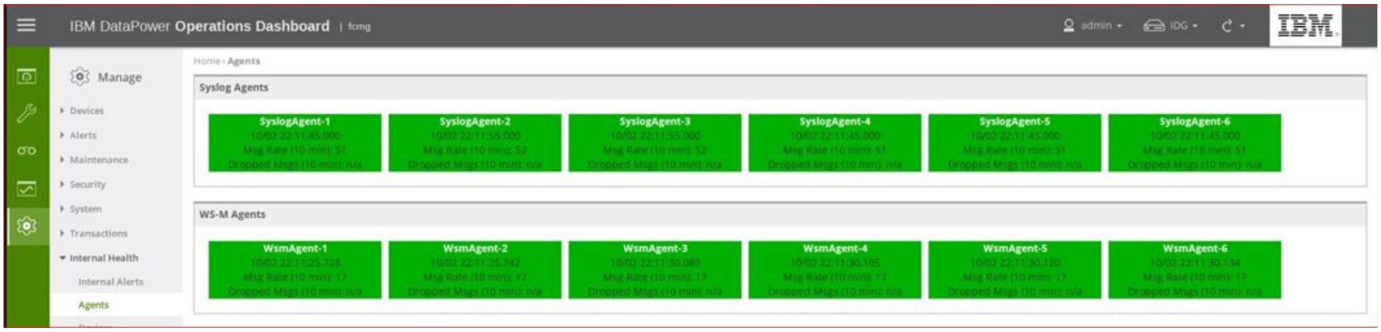
After a successful execution, you will be able to see the new federated cell member in the Manage System Nodes page.
For example, after federating cell member the page should look as follows:



System Nodes

ID	Name	Type	Agents IP	Agents DNS	
1	N001	MANAGEMENT	172.17.100.31		Edit
2	N002	DATA	172.17.100.33		Edit

Also, the new agents will be shown in the agents list in the Manage Internal Health Agents page.
For example, if the cell manager has two agents and there is a federated cell member with additional four agents, the page will show six agents:



Syslog Agents

SyslogAgent-1
10/02 22:11:45.000
Msg Rate (10 min): 51
Dropped Msgs (10 min): n/a

SyslogAgent-2
10/02 22:11:55.000
Msg Rate (10 min): 52
Dropped Msgs (10 min): n/a

SyslogAgent-3
10/02 22:11:55.000
Msg Rate (10 min): 52
Dropped Msgs (10 min): n/a

SyslogAgent-4
10/02 22:11:45.000
Msg Rate (10 min): 51
Dropped Msgs (10 min): n/a

SyslogAgent-5
10/02 22:11:45.000
Msg Rate (10 min): 51
Dropped Msgs (10 min): n/a

SyslogAgent-6
10/02 22:11:45.000
Msg Rate (10 min): 51
Dropped Msgs (10 min): n/a

WS-M Agents

WsmAgent-1
10/02 22:11:25.728
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

WsmAgent-2
10/02 22:11:25.742
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

WsmAgent-3
10/02 22:11:30.089
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

WsmAgent-4
10/02 22:11:30.105
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

WsmAgent-5
10/02 22:11:30.120
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

WsmAgent-6
10/02 22:11:30.134
Msg Rate (10 min): 17
Dropped Msgs (10 min): n/a

Configure the Monitored Device to the Federated Cell Member Agents

It is possible to configure entire monitored device or just a specific domain to the federated cell member's agents.

To configure monitored device / specific domain please follow instructions on Adding Monitored Devices.

Virtual Cell Environment Installation

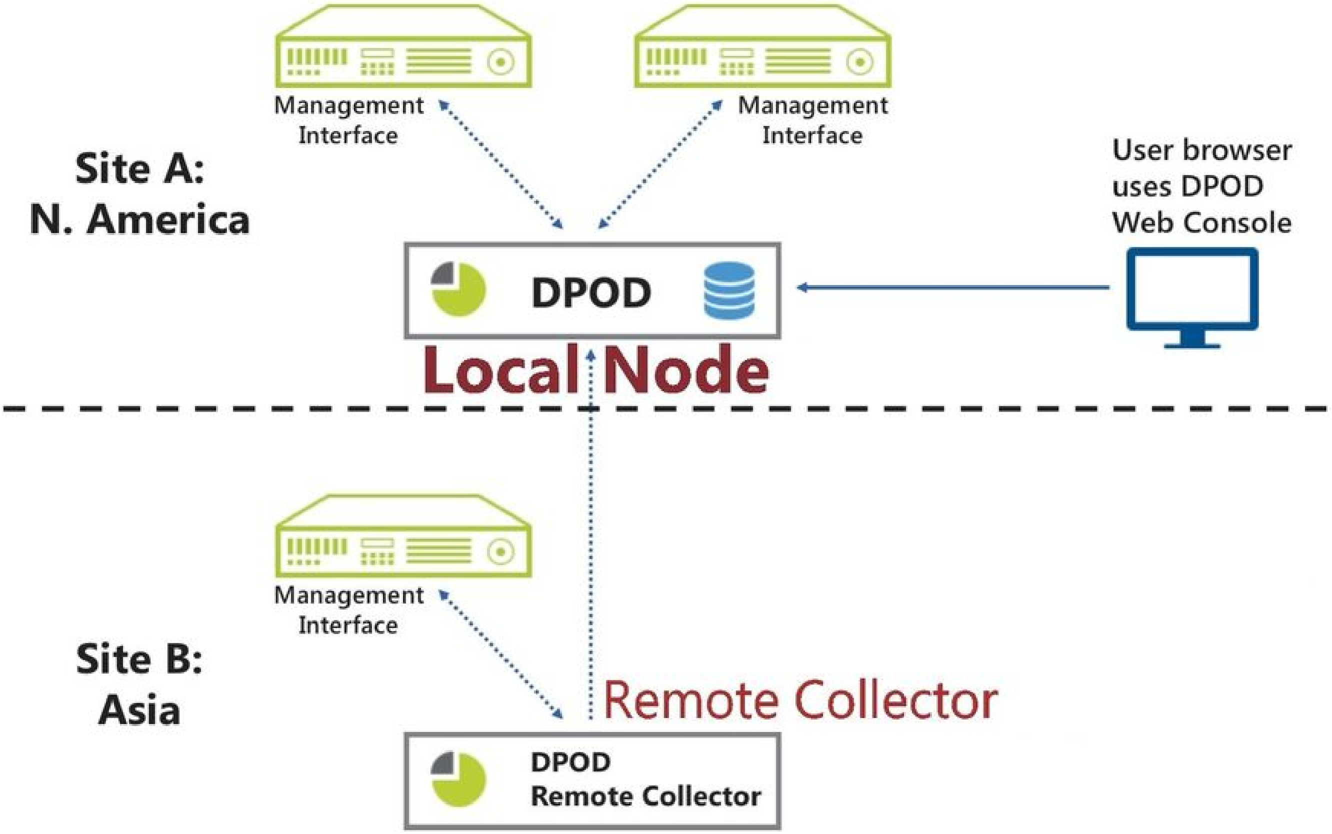
Prerequisites

1. Manager
    a. DPOD version 1.0.8.6 or above.
    b. Load configuration architecture: Medium or above (see: Hardware and Software Requirements)
    c. Non Appliance or Appliance
2. Members
    a. DPOD version 1.0.8.6 or above.
    b. The following mount points available: /data2,/data22,/data3,/data33,/data4,/data44 (see: Setup a Cell Environment)
    c. Load configuration architecture: Medium or above (see: Hardware and Software Requirements)
    d. Non Appliance only

Federation Process

1. Make sure network ports are open in the network firewall as described in Setup a Cell Environment Prerequisites (5):
2. Run the federation script from the manager server, once for each cell member, i.e.:

SETUP A REMOTE COLLECTOR



Overview

The remote collector deployment should assist in 2 scenarios:

- Data should be collected across several deployments but a consolidate single view is required (only one Local nodes is required).
- When a Local Node is reaching a CPU limit and an offload of work is required (can offload up to 20% CPU in high load).

In order to setup a new Remote Collector server you will need to install **another new DPOD server** based on the prerequisites below. The Node that will contain the Data and the console will be called "**Local Node**" and the second installation (contains only the Syslog and WS-M agent) will be called "**remote collector**".

Prerequisites

1. Two DPOD installations **must be** with the same version (minimum version is v1.0.7)
2. The remote collector DPOD installations should be configured with the "medium" architecture type as detailed in the Hardware and Software Requirements
3. Each installation will requires some different ports to be opened in the firewall - see table1
4. There are no requirements regarding the Environment name of each DPOD installation
5. The two DPODs need to be able to communicate with each other and with the monitored DataPower devices

Setup steps

In order to configure the local node and remote collector(s), run the following script **in the local node** once per remote collector .

```
configure_local_node.sh -a <IP address of the remote collector>
For example: configure_local_node.sh -a 192.168.0.5
```

The script will configure both the local node and remote collector.
Run this script once for each remote collector that you want to add - e.g. if you want to add two remote collectors, run the script twice (in the local node), first time with the IP address of the first remote collector, and second time with the IP of the second remote collector.

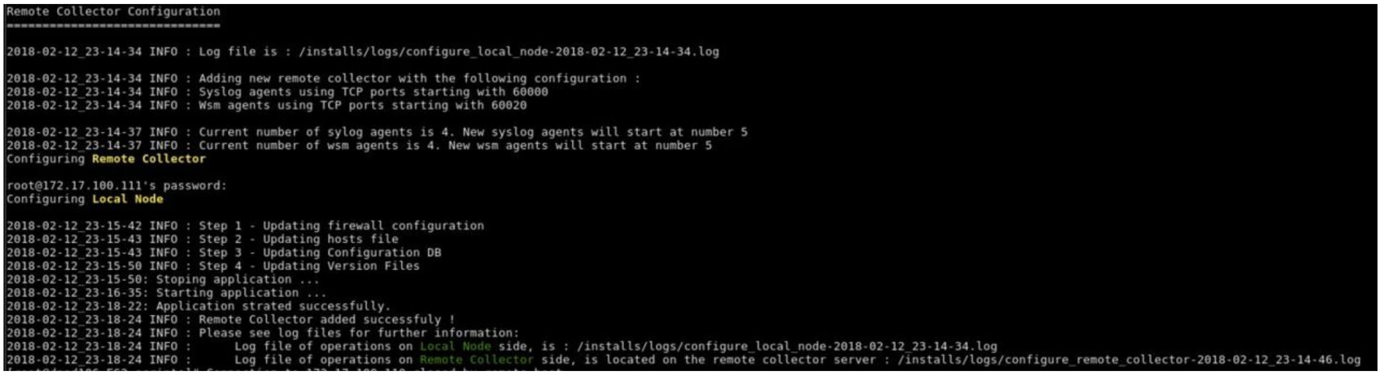
Optional parameters:

```
configure_local_node.sh -a <IP address of the remote collector> -s
<initial syslog agents port> -w <initial WSM agents port>
For example: configure_local_node.sh -a 192.168.0.5 -s 70000 -w 70050
```

The defaults are port 60000 for the initial syslog agents port and 60020 for the initial WSM agents port

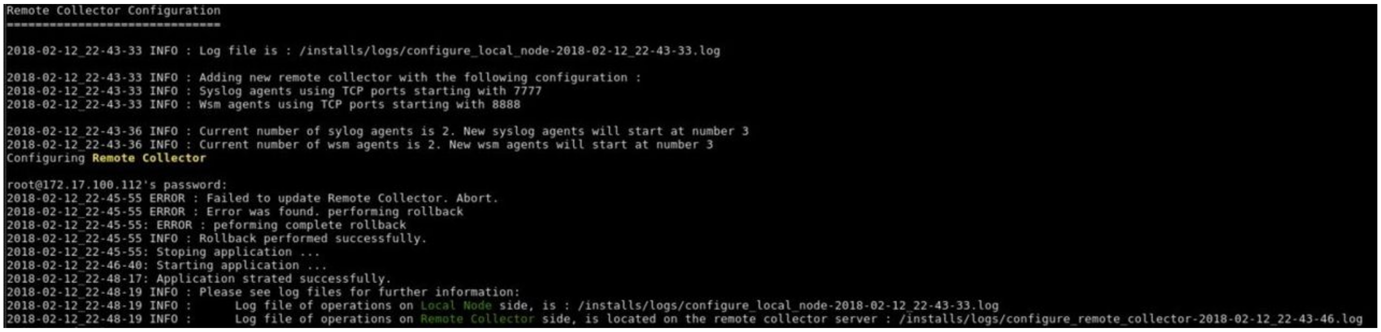
Output

Example for a successful execution - note that the script writes two log file, one in the local node and one in the remote collector, the log file names are mentioned in the script's output.



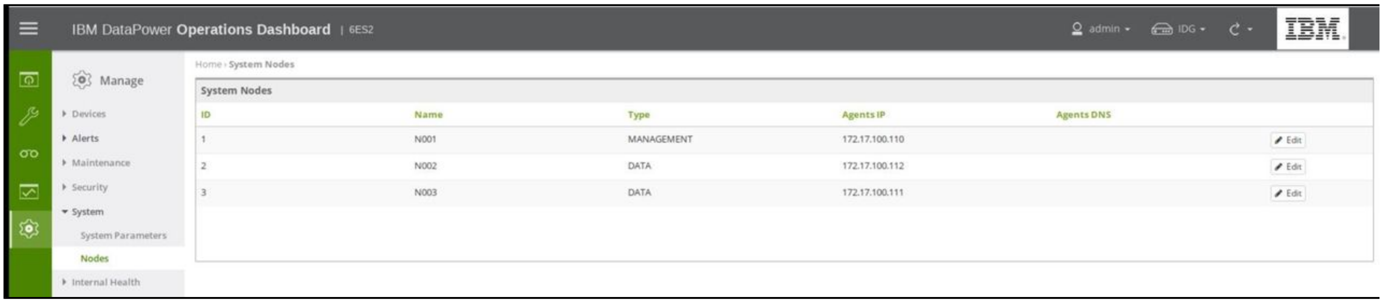
```
Remote Collector Configuration
==============================

2018-02-12_23-14-34 INFO : Log file is : /installs/logs/configure_local_node-2018-02-12_23-14-34.log

2018-02-12_23-14-34 INFO : Adding new remote collector with the following configuration :
2018-02-12_23-14-34 INFO : Syslog agents using TCP ports starting with 60000
2018-02-12_23-14-34 INFO : Wsm agents using TCP ports starting with 60020

2018-02-12_23-14-37 INFO : Current number of sylog agents is 4. New syslog agents will start at number 5
2018-02-12_23-14-37 INFO : Current number of wsm agents is 4. New wsm agents will start at number 5
Configuring Remote Collector

root@172.17.100.111's password:
Configuring Local Node

2018-02-12_23-15-42 INFO : Step 1 - Updating firewall configuration
2018-02-12_23-15-43 INFO : Step 2 - Updating hosts file
2018-02-12_23-15-43 INFO : Step 3 - Updating Configuration DB
2018-02-12_23-15-50 INFO : Step 4 - Updating Version Files
2018-02-12_23-15-50: Stoping application ...
2018-02-12_23-16-35: Starting application ...
2018-02-12_23-18-22: Application strated successfully.
2018-02-12_23-18-24 INFO : Remote Collector added successfuly !
2018-02-12_23-18-24 INFO : Please see log files for further information:
2018-02-12_23-18-24 INFO :      Log file of operations on Local Node side, is : /installs/logs/configure_local_node-2018-02-12_23-14-34.log
2018-02-12_23-18-24 INFO :      Log file of operations on Remote Collector side, is located on the remote collector server : /installs/logs/configure_remote_collector-2018-02-12_23-14-46.log
```

Example for a failed execution, you will need to check the log file for further information.
in case of a failure, the script will try to rollback the configuration changes it made, so you can try to fix the problem and run it again.



```
Remote Collector Configuration
==============================

2018-02-12_22-43-33 INFO : Log file is : /installs/logs/configure_local_node-2018-02-12_22-43-33.log

2018-02-12_22-43-33 INFO : Adding new remote collector with the following configuration :
2018-02-12_22-43-33 INFO : Syslog agents using TCP ports starting with 7777
2018-02-12_22-43-33 INFO : Wsm agents using TCP ports starting with 8888

2018-02-12_22-43-36 INFO : Current number of sylog agents is 2. New syslog agents will start at number 3
2018-02-12_22-43-36 INFO : Current number of wsm agents is 2. New wsm agents will start at number 3
Configuring Remote Collector

root@172.17.100.112's password:
2018-02-12_22-45-55 ERROR : Failed to update Remote Collector. Abort.
2018-02-12_22-45-55 ERROR : Error was found. performing rollback
2018-02-12_22-45-55: ERROR : peforming complete rollback
2018-02-12_22-45-55 INFO : Rollback performed successfully.
2018-02-12_22-45-55: Stoping application ...
2018-02-12_22-46-40: Starting application ...
2018-02-12_22-48-17: Application strated successfully.
2018-02-12_22-48-19 INFO : Please see log files for further information:
2018-02-12_22-48-19 INFO :      Log file of operations on Local Node side, is : /installs/logs/configure_local_node-2018-02-12_22-43-33.log
2018-02-12_22-48-19 INFO :      Log file of operations on Remote Collector side, is located on the remote collector server : /installs/logs/configure_remote_collector-2018-02-12_22-43-46.log
```

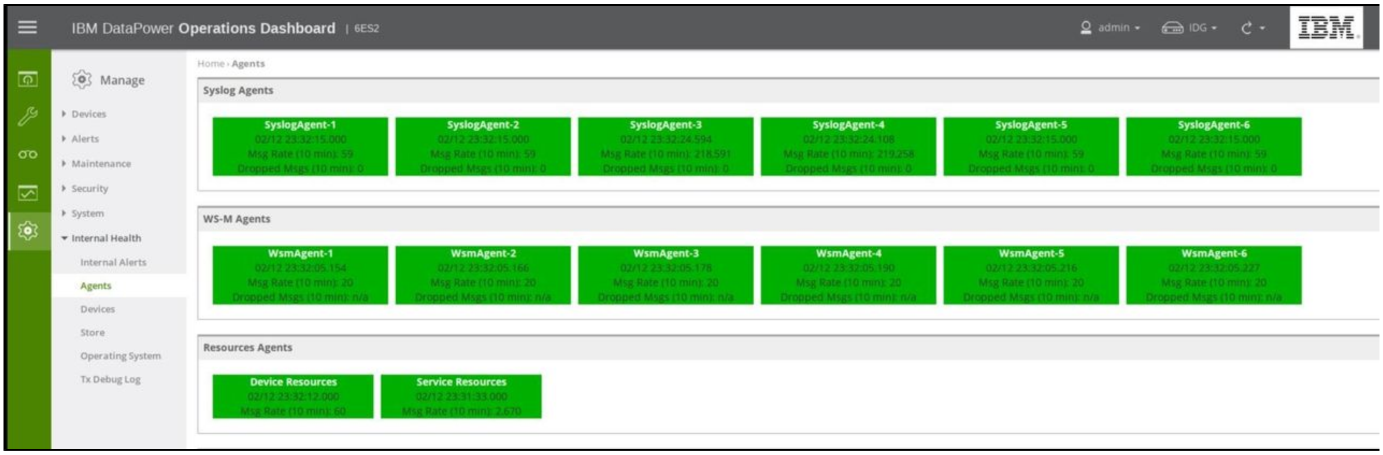
After a successful execution, you will be able to see the new remote collectors in the Manage System Nodes page,
For example, if we added two remote collectors:



System Nodes

ID	Name	Type	Agents IP	Agents DNS	
1	N001	MANAGEMENT	172.17.100.110		Edit
2	N002	DATA	172.17.100.112		Edit
3	N003	DATA	172.17.100.111		Edit

Also, the new agents will be shown in the agents in the Manage Internal Health Agents page.
For example, we have one local node with two agents and two remote collectors with two agents each, the page will show six agents:



Syslog Agents

SyslogAgent-1	SyslogAgent-2	SyslogAgent-3	SyslogAgent-4	SyslogAgent-5	SyslogAgent-6
02/12 23:32:15.000	02/12 23:32:15.000	02/12 23:32:24.594	02/12 23:32:24.108	02/12 23:32:15.000	02/12 23:32:15.000
Msg Rate (10 min): 59	Msg Rate (10 min): 59	Msg Rate (10 min): 218,591	Msg Rate (10 min): 219,258	Msg Rate (10 min): 59	Msg Rate (10 min): 59
Dropped Msgs (10 min): 0	Dropped Msgs (10 min): 0	Dropped Msgs (10 min): 0	Dropped Msgs (10 min): 0	Dropped Msgs (10 min): 0	Dropped Msgs (10 min): 0

WS-M Agents

WsmAgent-1	WsmAgent-2	WsmAgent-3	WsmAgent-4	WsmAgent-5	WsmAgent-6
02/12 23:32:05.154	02/12 23:32:05.166	02/12 23:32:05.178	02/12 23:32:05.190	02/12 23:32:05.216	02/12 23:32:05.227
Msg Rate (10 min): 20	Msg Rate (10 min): 20	Msg Rate (10 min): 20	Msg Rate (10 min): 20	Msg Rate (10 min): 20	Msg Rate (10 min): 20
Dropped Msgs (10 min): n/a	Dropped Msgs (10 min): n/a	Dropped Msgs (10 min): n/a	Dropped Msgs (10 min): n/a	Dropped Msgs (10 min): n/a	Dropped Msgs (10 min): n/a

Resources Agents

Device Resources	Service Resources
02/12 23:32:12.000	02/12 23:31:33.000
Msg Rate (10 min): 60	Msg Rate (10 min): 2,670

Configure The Monitored Device to Remote Collector's Agents

It is possible to configure entire monitored device to remote collector's agent or just a specific domain.

To configure monitored device / specific domain please follow instructions on Adding Monitored Devices

Manual Setup Steps

> We recommend using the script described in the previous section.
> There is no need to take any manual steps if you already run the script.

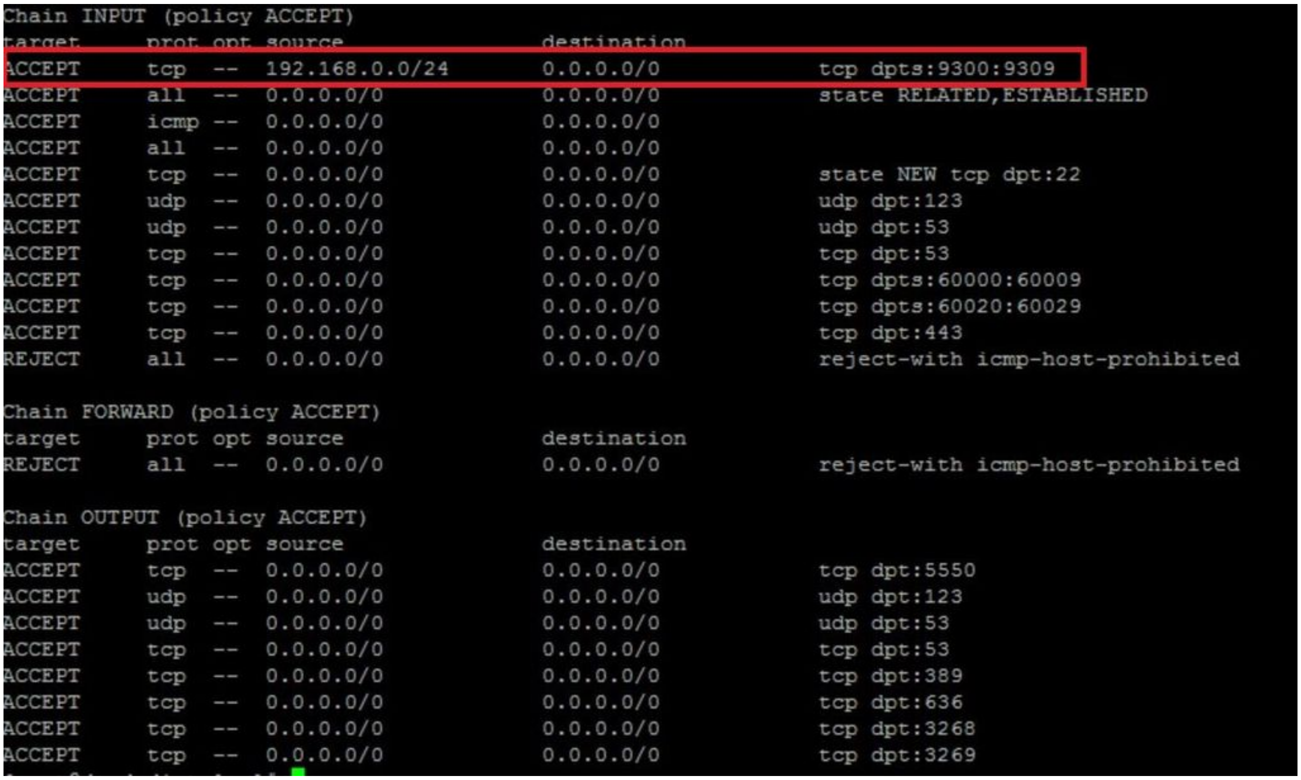
1. The following communication and ports are used in a remote collector deployment scenario (table 1). Perform the following commands to accomplish this task on each DPOD local firewall:

   Run in **Local Node -**
   Change the XXXX to the IP of the **Remote Collector**

   ```
   iptables -I INPUT -p tcp -s XXXX/24 --dport 9300:9309 -j ACCEPT
   service iptables save
   service iptables restart
   ```

   After running the commands, run the following command and search the output for two entries showing port 9300 (shown in red in the below screenshot)

   ```
   iptables -L -n
   ```



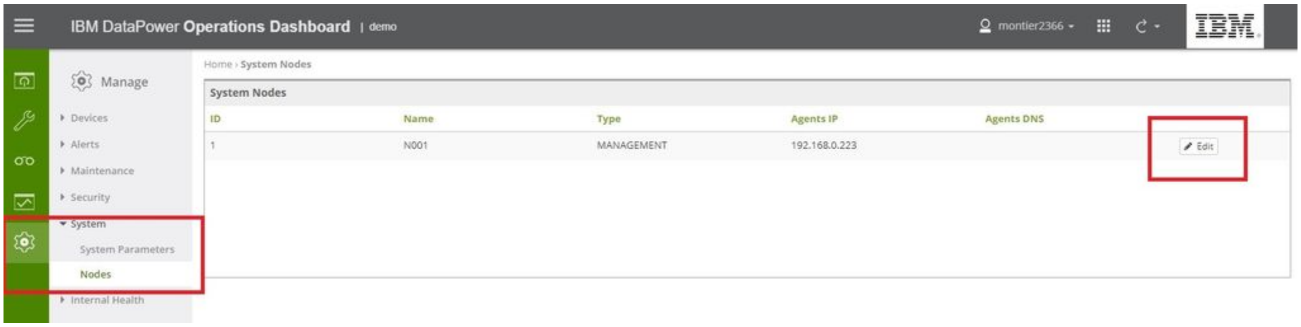
```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.0/24       0.0.0.0/0            tcp dpts:9300:9309
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:123
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpts:60000:60009
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpts:60020:60029
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:443
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:5550
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:123
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:389
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:636
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3268
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:3269
```

table 1

From	To	Ports (Defaults)	Protocol	Usage
Local Node DPOD Appliance	Each Monitored Device	5550 (TCP)	HTTP/S	Monitored Device administration management interface
Local Node DPOD Appliance	DNS Server	TCP and UDP 53	DNS	DNS services
Local Node DPOD Appliance	NTP Server	123 (UDP)	NTP	Time synchronization
Local Node DPOD Appliance	Organizational mail server	25 (TCP)	SMTP	Send reports by email
Local Node DPOD Appliance	LDAP	TCP 389 / 636 (SSL). TCP 3268 / 3269 (SSL)	LDAP	Authentication & authorization. Can be over SSL
NTP Server	Local Node DPOD Appliance	123 (UDP)	NTP	Time synchronization
Each Monitored Device	Local Node DPOD Appliance	60000-60009 (TCP)	TCP	SYSLOG Data
Each Monitored Device	Local Node DPOD Appliance	60020-60029 (TCP)	HTTP/S	WS-M Payloads
FROM Users IPs	Local Node DPOD Appliance	443 (TCP)	HTTP/S	Access to with IBM DataPower Operations Dashboard Console
FROM Admins IPs	Local Node DPOD Appliance	22 (TCP)	TCP	SSH
Remote Collector DPOD Appliance	Local Node DPOD Appliance	9300-9309	TCP	DPOD's Store communication
Remote Collector DPOD Appliance	Each Monitored Device	5550 (TCP)	HTTP/S	Monitored Device administration management interface

Remote Collector DPOD Appliance	DNS Server	TCP and UDP 53	DNS	DNS services
Remote Collector DPOD Appliance	NTP Server	123 (UDP)	NTP	Time synchronization
Remote Collector DPOD Appliance	Organizational mail server	25 (TCP)	SMTP	Send reports by email
Remote Collector DPOD Appliance	LDAP	TCP 389 / 636 (SSL). TCP 3268 / 3269 (SSL)	LDAP	Authentication & authorization. Can be over SSL
NTP Server	Remote Collector DPOD Appliance	123 (UDP)	NTP	Time synchronization
Each Monitored Device	Remote Collector DPOD Appliance	60000-60009 (TCP)	TCP	SYSLOG Data
Each Monitored Device	Remote Collector DPOD Appliance	60020-60029 (TCP)	HTTP/S	WS-M Payloads
FROM Users IPs	Remote Collector DPOD Appliance	443 (TCP)	HTTP/S	Access to with IBM DataPower Operations Dashboard Console
FROM Admins IPs	Remote Collector DPOD Appliance	22 (TCP)	TCP	SSH

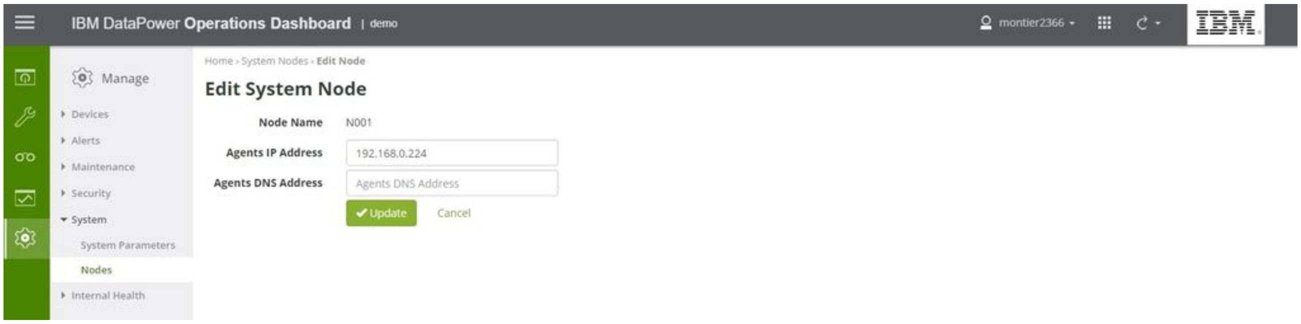
2. From the **Local Node's** UI, go to the Manage menu, select "Nodes" under "System" and click "Edit"



System Nodes

ID	Name	Type	Agents IP	Agents DNS	
1	N001	MANAGEMENT	192.168.0.223		Edit

Enter the IP address of the **Remote Collector** device and click "Update", you can leave the "Agents DNS Address" empty



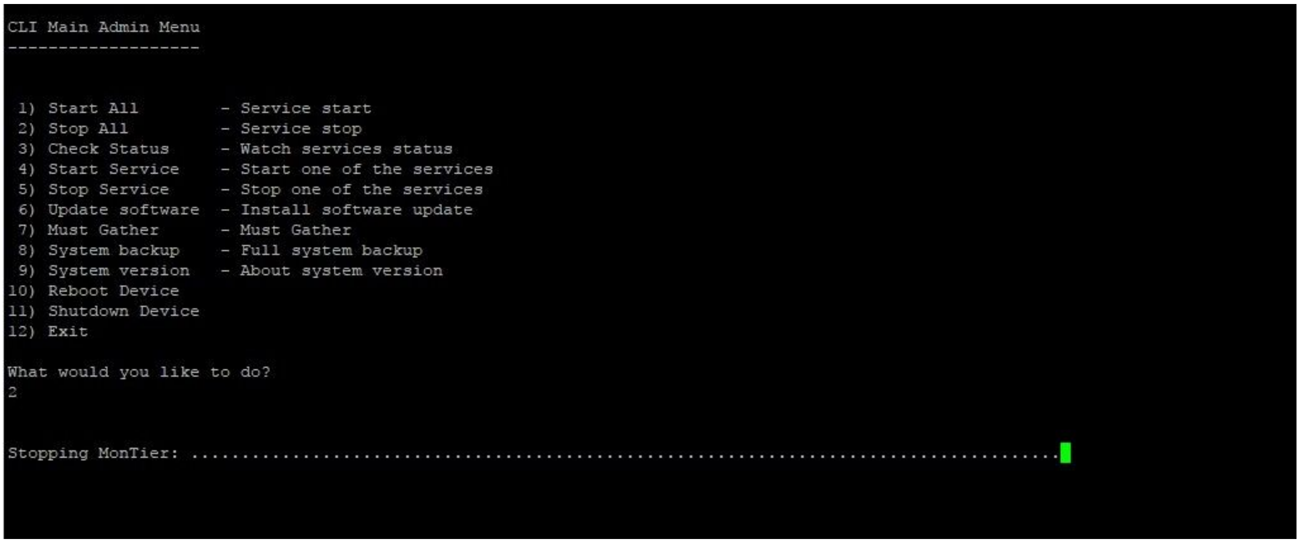
Edit System Node

Node Name N001

Agents IP Address 192.168.0.224

Agents DNS Address Agents DNS Address

3. In the **Local Node**
Connect to the **Local Node** DPOD via ssh as root user (using putty or any other ssh client)
Using the Command Line Interface choose option 2 - "Stop All", and wait until all the services are stopped, this may take a few minutes to complete.



```
CLI Main Admin Menu
-------------------


 1) Start All        - Service start
 2) Stop All         - Service stop
 3) Check Status     - Watch services status
 4) Start Service    - Start one of the services
 5) Stop Service     - Stop one of the services
 6) Update software  - Install software update
 7) Must Gather      - Must Gather
 8) System backup    - Full system backup
 9) System version   - About system version
10) Reboot Device
11) Shutdown Device
12) Exit

What would you like to do?
2


Stopping MonTier: .....................................................................................
```

4. In the **Local Node**
   Using putty or any other ssh client, issue the following command:

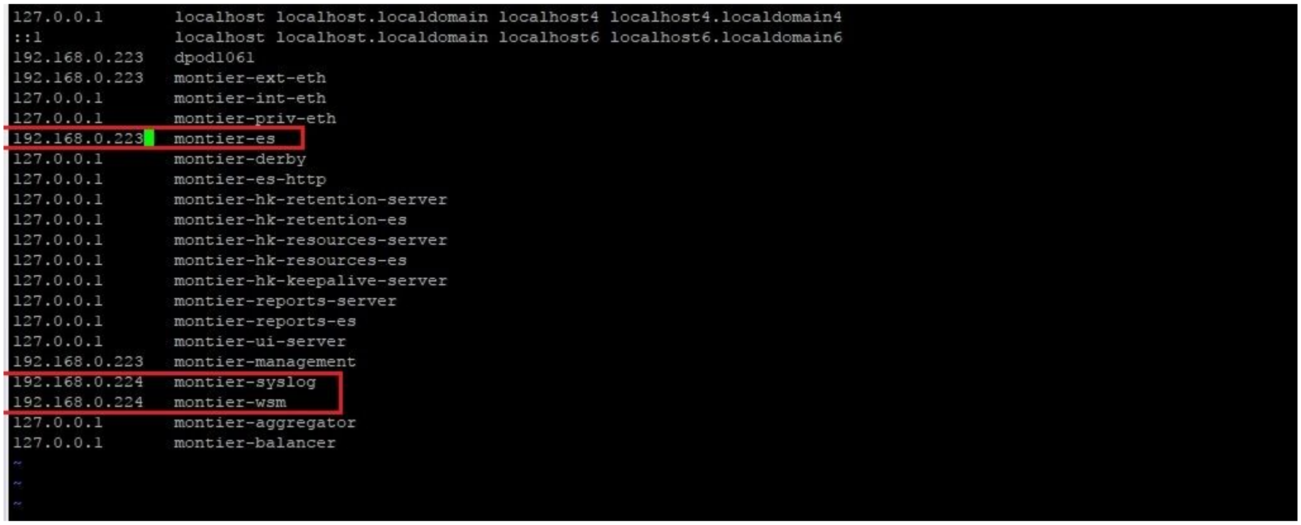
```
sed -i -e "s/^SERVICES_SIXTH_GROUP=\".*MonTier-SyslogAgent-1
MonTier-HK-WdpServiceResources
MonTier-HK-WdpDeviceResources/SERVICES_SIXTH_GROUP=\"MonTier-HK-Wdp
ServiceResources MonTier-HK-WdpDeviceResources/g"
/etc/sysconfig/MonTier
```

5. In the **Local Node**
   Using putty or any other ssh client, issue the following command:

```
mv /etc/init.d/MonTier-SyslogAgent-1
/etc/init.d/Disabled-MonTier-SyslogAgent-1
mv /etc/init.d/MonTier-SyslogAgent-2
/etc/init.d/Disabled-MonTier-SyslogAgent-2
mv /etc/init.d/MonTier-SyslogAgent-3
/etc/init.d/Disabled-MonTier-SyslogAgent-3
mv /etc/init.d/MonTier-SyslogAgent-4
/etc/init.d/Disabled-MonTier-SyslogAgent-4
mv /etc/init.d/MonTier-SyslogAgent-5
/etc/init.d/Disabled-MonTier-SyslogAgent-5
mv /etc/init.d/MonTier-SyslogAgent-6
/etc/init.d/Disabled-MonTier-SyslogAgent-6
mv /etc/init.d/MonTier-SyslogAgent-7
/etc/init.d/Disabled-MonTier-SyslogAgent-7
mv /etc/init.d/MonTier-SyslogAgent-8
/etc/init.d/Disabled-MonTier-SyslogAgent-8
mv /etc/init.d/MonTier-SyslogAgent-9
/etc/init.d/Disabled-MonTier-SyslogAgent-9
mv /etc/init.d/MonTier-SyslogAgent-10
/etc/init.d/Disabled-MonTier-SyslogAgent-10


mv /etc/init.d/MonTier-WsmAgent-1
/etc/init.d/Disabled-MonTier-WsmAgent-1
mv /etc/init.d/MonTier-WsmAgent-2
/etc/init.d/Disabled-MonTier-WsmAgent-2
mv /etc/init.d/MonTier-WsmAgent-3
/etc/init.d/Disabled-MonTier-WsmAgent-3
mv /etc/init.d/MonTier-WsmAgent-4
/etc/init.d/Disabled-MonTier-WsmAgent-4
mv /etc/init.d/MonTier-WsmAgent-5
/etc/init.d/Disabled-MonTier-WsmAgent-5
```

Note: some errors might appear for services that are not exists in your specific deployment architecture type - for example "mv: cannot stat '/etc/init.d/Disabled-MonTier-SyslogAgent-10': No such file or directory"

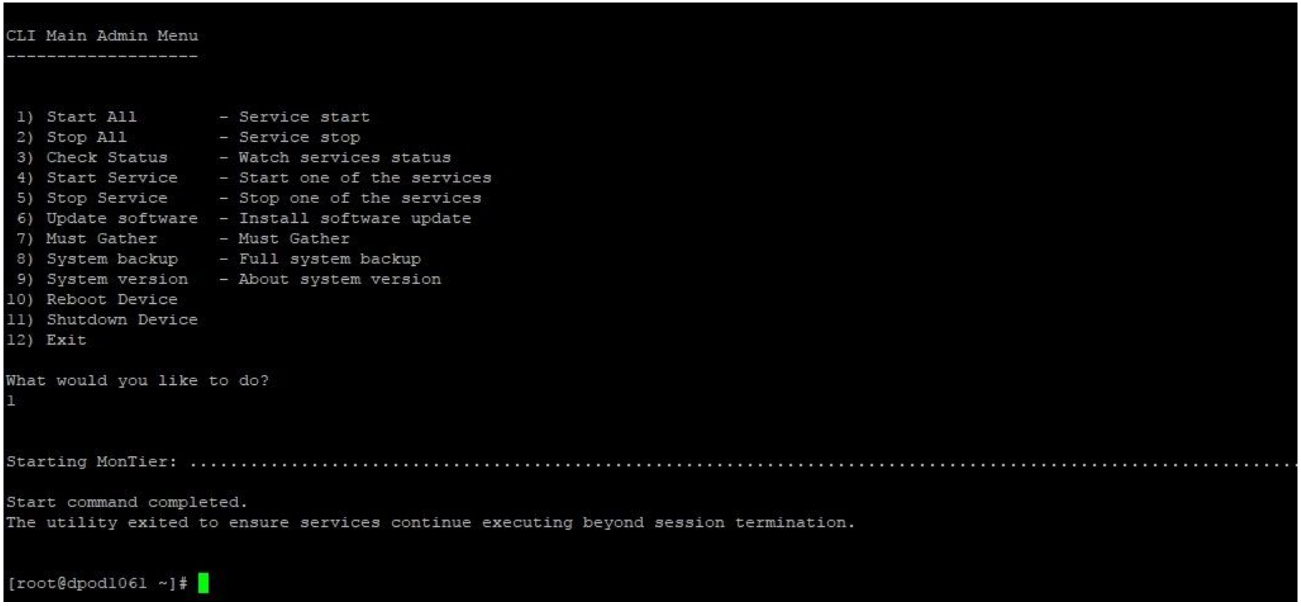
6. In the **Local Node**
   Using any text editor (like vi), edit /etc/hosts files (e.g. vi /etc/hosts)
   Change the following entries:
   montier-es from 127.0.0.1 to the IP of the **Local node** device
   montier-syslog and **montier-wsm** to the IP of the **remote collector** device



```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1             localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.0.223   dpod1061
192.168.0.223   montier-ext-eth
127.0.0.1       montier-int-eth
127.0.0.1       montier-priv-eth
192.168.0.223   montier-es
127.0.0.1       montier-derby
127.0.0.1       montier-es-http
127.0.0.1       montier-hk-retention-server
127.0.0.1       montier-hk-retention-es
127.0.0.1       montier-hk-resources-server
127.0.0.1       montier-hk-resources-es
127.0.0.1       montier-hk-keepalive-server
127.0.0.1       montier-reports-server
127.0.0.1       montier-reports-es
127.0.0.1       montier-ui-server
192.168.0.223   montier-management
192.168.0.224   montier-syslog
192.168.0.224   montier-wsm
127.0.0.1       montier-aggregator
127.0.0.1       montier-balancer
~
~
~
```

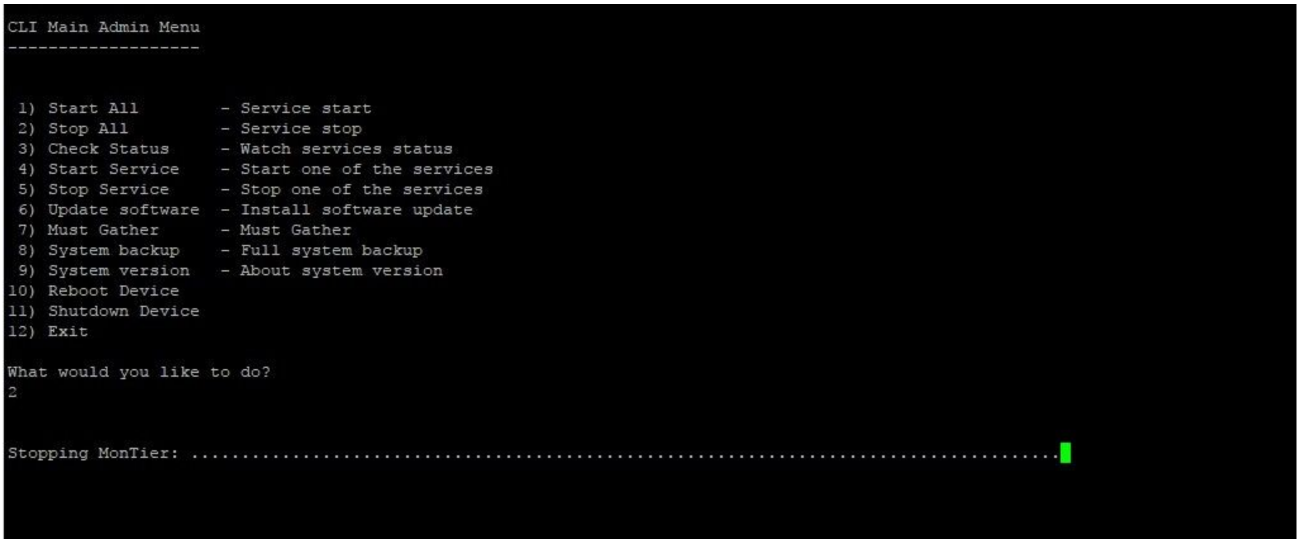
you should save the changes when exit (e.g wq)

7. In the **Local Node**
   Using the Command Line Interface - Select option 1 **"Start All"**, this may take a few minutes to complete



```
CLI Main Admin Menu
-------------------


 1) Start All        - Service start
 2) Stop All         - Service stop
 3) Check Status     - Watch services status
 4) Start Service    - Start one of the services
 5) Stop Service     - Stop one of the services
 6) Update software  - Install software update
 7) Must Gather      - Must Gather
 8) System backup    - Full system backup
 9) System version   - About system version
10) Reboot Device
11) Shutdown Device
12) Exit

What would you like to do?
1


Starting MonTier: ..............................................................................................

Start command completed.
The utility exited to ensure services continue executing beyond session termination.


[root@dpod1061 ~]#
```

8. Connect to the **Remote Collector** DPOD via ssh as root user (using putty or any other ssh client)
   Using the Command Line Interface choose option 2 - "Stop All", and wait until all the services are stopped, this may take a few minutes to complete.



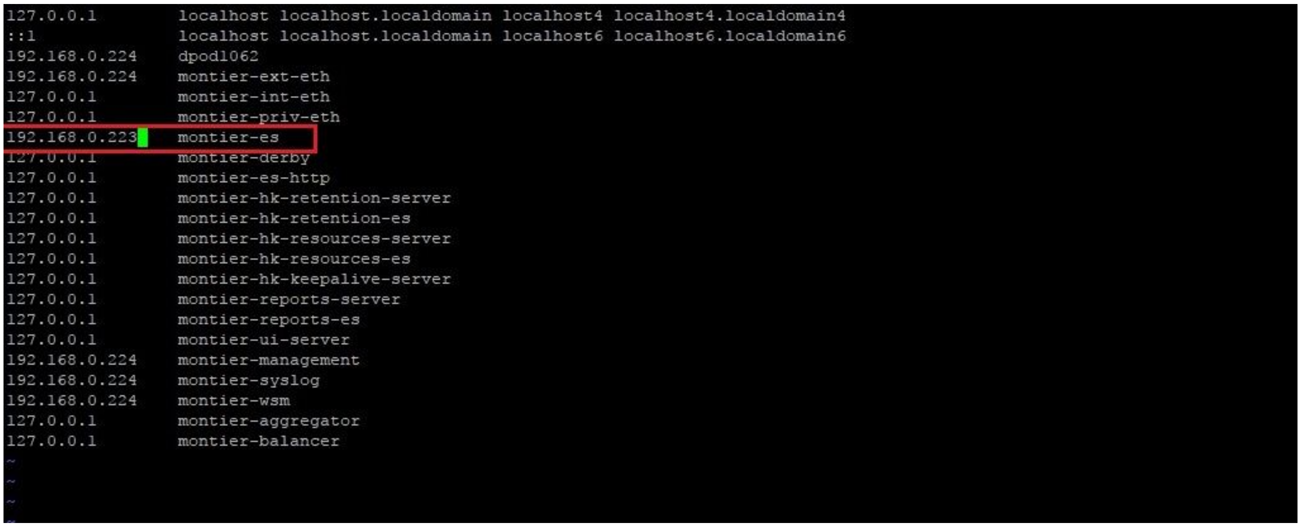
```
CLI Main Admin Menu
-------------------


 1) Start All        - Service start
 2) Stop All         - Service stop
 3) Check Status     - Watch services status
 4) Start Service    - Start one of the services
 5) Stop Service     - Stop one of the services
 6) Update software  - Install software update
 7) Must Gather      - Must Gather
 8) System backup    - Full system backup
 9) System version   - About system version
10) Reboot Device
11) Shutdown Device
12) Exit

What would you like to do?
2


Stopping MonTier: ......................................................................................
```

9. In the **Remote Collector**
   Using putty or any other ssh client, issue the following commands:

```
mv /etc/init.d/MonTier-es-raw-trans-Node-1
/etc/init.d/Disabled-MonTier-es-raw-trans-Node-1
mv /etc/init.d/MonTier-es-raw-trans-Node-2
/etc/init.d/Disabled-MonTier-es-raw-trans-Node-2
mv /etc/init.d/MonTier-es-raw-trans-Node-3
/etc/init.d/Disabled-MonTier-es-raw-trans-Node-3
mv /etc/init.d/MonTier-es-raw-trans-Node-4
/etc/init.d/Disabled-MonTier-es-raw-trans-Node-4

mv /etc/init.d/MonTier-Derby /etc/init.d/Disabled-MonTier-Derby

mv /etc/init.d/MonTier-HK-ESRetention
/etc/init.d/Disabled-MonTier-HK-ESRetention

mv /etc/init.d/MonTier-HK-SyslogKeepalive
/etc/init.d/Disabled-MonTier-HK-SyslogKeepalive
mv /etc/init.d/MonTier-HK-WsmKeepalive
/etc/init.d/Disabled-MonTier-HK-WsmKeepalive

mv /etc/init.d/MonTier-HK-WdpDeviceResources
/etc/init.d/Disabled-MonTier-HK-WdpDeviceResources
mv /etc/init.d/MonTier-HK-WdpServiceResources
/etc/init.d/Disabled-MonTier-HK-WdpServiceResources

mv /etc/init.d/MonTier-Reports /etc/init.d/Disabled-MonTier-Reports

mv /etc/init.d/MonTier-UI /etc/init.d/Disabled-MonTier-UI

sed -i -e
"s/^SERVICES_FIRST_GROUP=\".*/SERVICES_FIRST_GROUP=\"\"/g"
/etc/sysconfig/MonTier
sed -i -e
"s/^SERVICES_SECOND_GROUP=\".*/SERVICES_SECOND_GROUP=\"\"/g"
/etc/sysconfig/MonTier
sed -i -e
"s/^SERVICES_THIRD_GROUP=\".*/SERVICES_THIRD_GROUP=\"\"/g"
/etc/sysconfig/MonTier
sed -i -e "s/\MonTier-HK-WdpServiceResources
MonTier-HK-WdpDeviceResources//g" /etc/sysconfig/MonTier
sed -i -e
"s/^SERVICES_SEVENTH_GROUP=\".*/SERVICES_SEVENTH_GROUP=\"\"/g"
/etc/sysconfig/MonTier
```

Note: some errors might appear for services that are not exists in your specific deployment architecture type - for example "mv: cannot stat ‘/etc/init.d/MonTier-es-raw-trans-Node-4’: No such file or directory"

10. In the **Remote Collector**
Using any text editor (like vi), edit /etc/hosts files (e.g. vi /etc/hosts)
Change the following entries:
montier-es from 127.0.0.1 to the ip of the **Local Node** device



```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain4
::1             localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.0.224   dpod1062
192.168.0.224   montier-ext-eth
127.0.0.1       montier-int-eth
127.0.0.1       montier-priv-eth
192.168.0.223   montier-es
127.0.0.1       montier-derby
127.0.0.1       montier-es-http
127.0.0.1       montier-hk-retention-server
127.0.0.1       montier-hk-retention-es
127.0.0.1       montier-hk-resources-server
127.0.0.1       montier-hk-resources-es
127.0.0.1       montier-hk-keepalive-server
127.0.0.1       montier-reports-server
127.0.0.1       montier-reports-es
127.0.0.1       montier-ui-server
192.168.0.224   montier-management
192.168.0.224   montier-syslog
192.168.0.224   montier-wsm
127.0.0.1       montier-aggregator
127.0.0.1       montier-balancer
~
~
~
~
```

11. In the **Remote Collector**
    Using the Command Line Interface choose option 1 - "Start All", and wait until all the services are stopped, this may take a few minutes to complete.

12. Verify in the console in Management Internal health Agents that all agents are in green state.

13. Run the following two scripts, you will need to obtain them from IBM support:
    in the **Local Node -** configure_local_node.sh
    in the **Remote Collector** - configure_remote_collector.sh
14. In the **Local Node - !! Only if DPOD was already attached to DataPower Gateways !!**
    you will need to reconfigure again all the the attached device.

After the setup is complete - DPOD's web console will not longer be available for the **Remote Collector,** The only way to connect to the **Remote Collector** will be via ssh client

Upgrade

DPOD software updates are available from time to time and include enhancements, security updates, component upgrade, bug fixes etc.

Up to version 1.0.8.0, each DPOD fix pack file is not including any previous fix pack. For example: to upgrade from v1.0.5 to v1.0.7 you will need to first upgrade to v1.0.6 with the downloaded fix of v106 and after a successful upgrade to v106 you may apply the fix to v107.

DPOD installation from version 1.0.8.0 and above can apply the latest fix available in fix central. For example: to upgrade from v1.0.7 to latest you will need to first upgrade to v1.0.8 with the downloaded fix of v108 and after a successful upgrade apply the latest fix from fix central.

Additional RPM packages need to be installed when upgrading a non appliance DPOD installation from a version prior to v1.0.9.0.
Please make sure the following packages are installed before running the upgrade: **httpd, mod_ssl, curl, wget, unzip, iptables, iptables-services, bc, fontconfig**

The following sections describe the process of upgrading an existing installation.

> To upgrade a **Cell environment** - first stop DPOD on the Cell Manager and on all Cell Members, then upgrade the Cell Members, and only after all Cell Members have been upgraded, upgrade the Cell Manager.

OBTAIN THE SOFTWARE UPDATE

DPOD software updates are available through IBM fix central.

The download consists of two types of files :

1. The update file in the format of : DPOD-fixpack-<version number>.sfs (for example: DPOD-fixpack-1_0_8_5.sfs)
2. The md5 hash calculation of the update file : DPOD-fixpack-<version number>.md5 (for example: DPOD-fixpack-1_0_8_5.md5)

MAKE SURE SQUASHFS SUPPORT (ONLY FOR NON APPLIANCE INSTALLATION)

Make sure the update file can be mounted (squashfs support) using the following command

```
lsmod | grep squash

expected output :
squashfs
```

COPY THE SOFTWARE UPDATE TO THE DPOD SERVER

Copy the update files to the following directory on the DPOD server :

```
/installs/update/fix/TODO
```

If the directory is missing for some reason, please re create it :

```
mkdir -p /installs/update/fix/TODO
```

MAKE SURE THERE IS ENOUGH DISK SPACE

The software update requirements for available disk space may change from version to version. See version table below.

The disk space is needed at the "/installs" mount point and can be displayed using the following command:

```
df -h /installs

Output example:
Filesystem                    Size  Used Avail Use% Mounted on
/dev/mapper/vg_inst-lv_inst  7.0G  5.5G  1.6G  79% /installs
```

During the software update installation, the internal configuration database is being backed-up. The backup requires additional available disk space on the "/installs" mount point.

To calculate the needed available disk space for the internal configuration database backup please use the following command (**in this example DB size is 43MB**):

```
du -ksh /app/derby/

Output example:
43M     /app/derby/
```

See the following table for needed available disk space on "/installs" for the software update:

Version	Needed Available Disk Space
1.0.3	700MB + DB SIZE
1.0.4	700MB + DB SIZE
1.0.5	2500MB + DB SIZE
1.0.6	700MB + DB SIZE
1.0.7	3000MB + DB SIZE
1.0.8	2000MB + DB SIZE

If there is not enough free disk space on the "/installs" mount point the user may free some by deleting files from the following directories :

Directory	Description
/installs/update/fix/TODO	Remove old DPOD update files (.sfs)
/installs/update/fix/backups	Remove old DPOD backup directories
/installs/APPL-setup	Remove DPOD installation file

Version 1.0.9 and above also requires at least 100MB free space at the root ("/") mount point.

INSTALL THE SOFTWARE UPDATE

A technical issue prevents upgrading DPOD installations that were installed using **version 1.0.2.0 ISO file**.
Before upgrading an 1.0.2.0 ISO-based DPOD installation to a newer version, please run the following command from a console / ssh session:
cd /installs
rm -rf dev-tools

> To identify the ISO version used for your installation, please run the CLI Admin utility (app-util.sh) and select option 9 (system version). The version appears in the ISO file name next to the "package_name" attribute, for example: ibm-DPOD-STD-APPL-**1.0.2.0**-2016-11-15_03_50_10_731-IST-BLD212.iso

Run the following command from the location you downloaded the update files to.

```
MonTierUpdateInstaller.sh -u DPOD-update-<version number>.sfs -s
DPOD-update-<version number>.md5
```

For example:

```
MonTierUpdateInstaller.sh -u DPOD-update-1_3_0.sfs -s
DPOD-update-1_3_0.md5
```

You may encounter the following message:

```
INFO file MonTierUpdateInstaller.sh was updated successfully.
INFO important !!! Please run MonTierUpdateInstaller.sh again.
```

This message means that the MonTierUpdateInstaller.sh was updated and you should rerun the command.
After running the command again you will be prompted to confirm the software update process. press "Y" to confirm or "N" to abort.

```
Software update :

   Please DO NOT interrupt during the process !

   Are you sure you want to continue ? [y/n]
```

When the software update level is not compatible with the current system version you will receive the following message on the console output :

```
error, software update can NOT be applied to this system version.
aborting update...
```

> Do Not interrupt the software update process after it has begun

When the software update completes, the system will display the following messages on the console output.

```
Starting software update. log file is
/installs/update/fix/logs/montier-update-2016-08-01_16-13-35.log
stopping application ...
application stopped successfully.
starting software update.....
updated complete successfully
starting application ...
application strated successfully.
update DPOD-update-1_3_0.sfs was installed successfully. log file
/installs/update/fix/logs/montier-update-2016-08-01_16-13-35.log
```

Please review the upgrade log file if the console displays any error messages.

MANUAL POST UPDATE INSTALLATION

Important: After the upgrade is complete, Syslog must be manually re-configured on all monitored devices using the Web Console (under Manage Monitored Devices).

For more details, please see the section "Configure The New Monitored Device" in Adding Monitored Devices.

Upgrade to v1.0.5.0 - Special Steps

DPOD software updates are available from time to time and include enhancements, security updates, component upgrade, bug fixes etc.
The following sections describe the process of upgrading an existing installation.

Obtain the software update

DPOD software updates are available through IBM fix central.

The download consists of two types of files :

1. The update file in the format of : DPOD-fixpack-<version number>.sfs (for example: DPOD-fixpack-1_0_5.sfs)
2. The md5 hash calculation of the update file : DPOD-update-<version number>.md5

Copy the software update to the DPOD server

Copy the update files to the following directory on the DPOD server :

```
/installs/update/fix/TODO
```

If the directory is missing for some reason, please re create it :

```
mkdir -p /installs/update/fix/TODO
```

Install the software update

Run the following command from the location you downloaded the update files to.

```
MonTierUpdateInstaller.sh -u DPOD-update-<version number>.sfs -s
DPOD-update-<version number>.md5
```

For example:

```
MonTierUpdateInstaller.sh -u DPOD-update-1_5_0.sfs -s
DPOD-update-1_5_0.md5
```

After running the command you will be prompted to confirm the software update process. press "Y" to confirm or "N" to abort.

```
Software update :

   Please DO NOT interrupt during the process !

   Are you sure you want to continue ? [y/n]
```

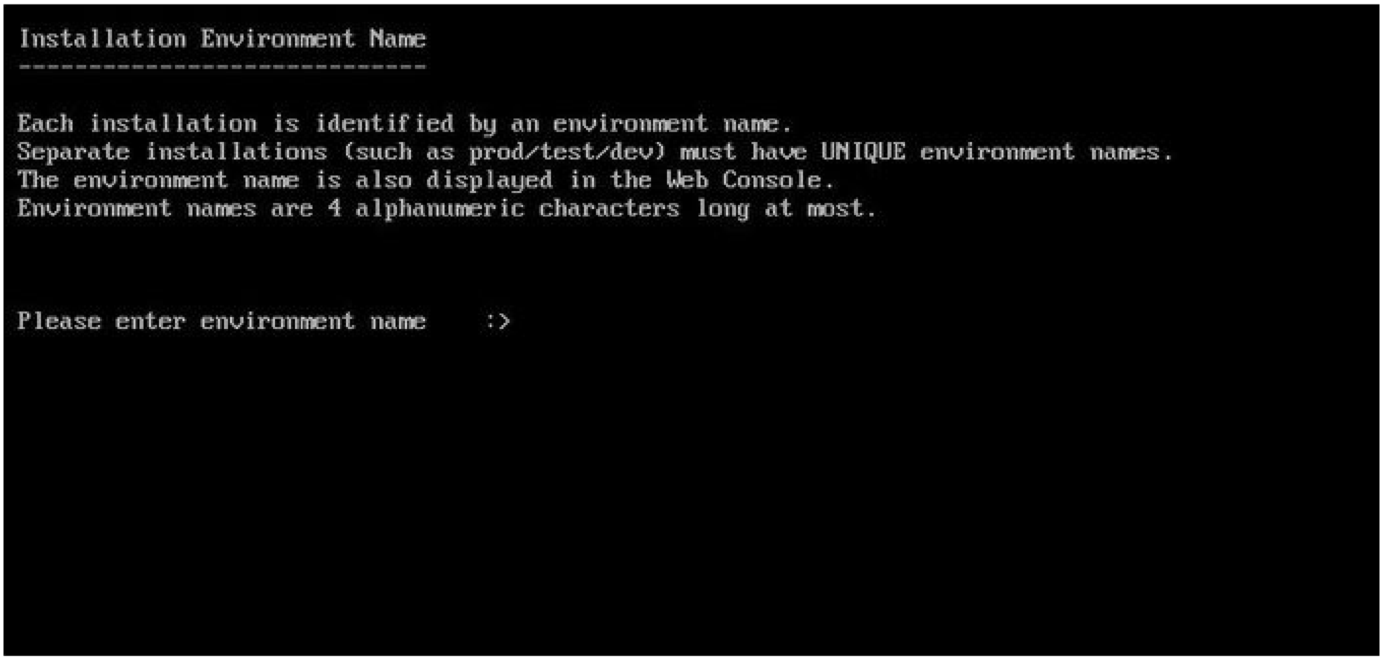
When the software update level is not compatible with the current system version you will receive the following message on the console output :

```
error, software update can NOT be applied to this system version.
aborting update...
```

Do Not interrupt the software update process after it has begun

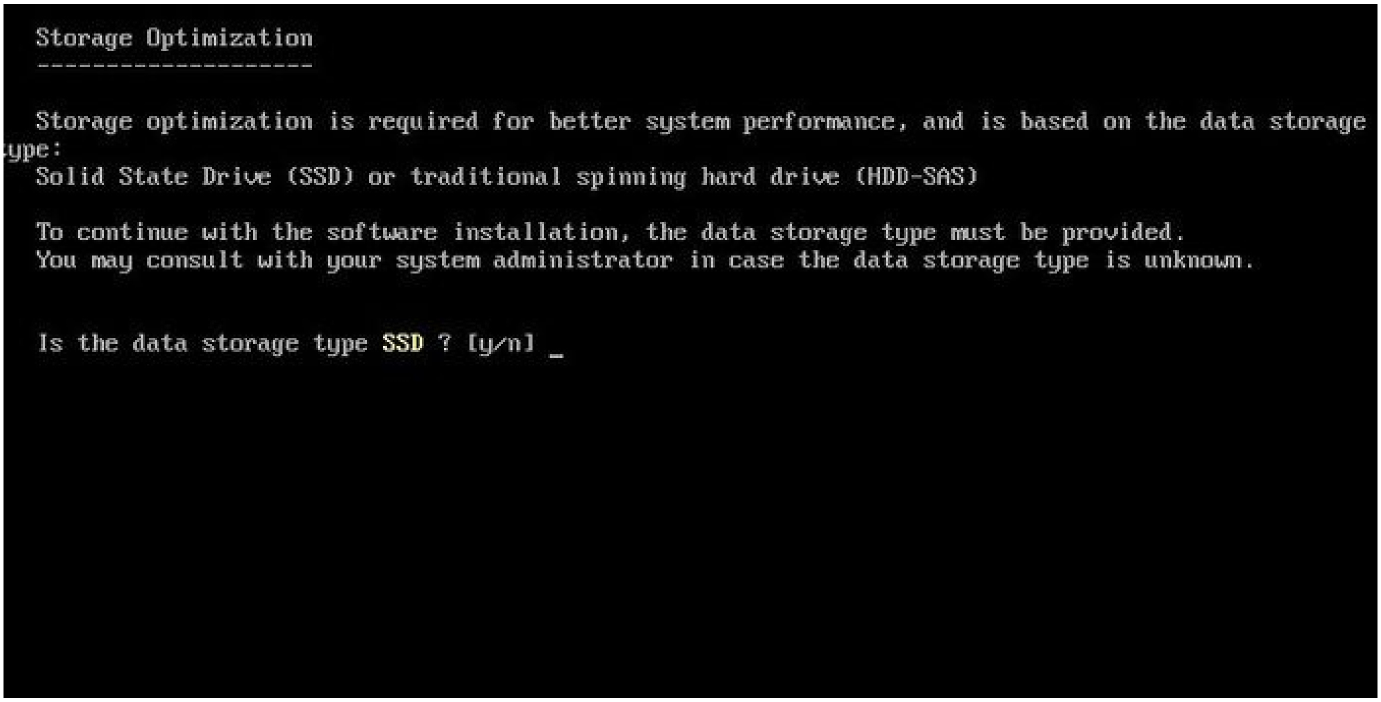
Choose an environment name for this DPOD installation, each DPOD installation must have a **unique** 4-character environment name

If you are installing a second DPOD machine that will be used as the standby machine in a DR Active/Standby scenario, the environment name must be identical to the environment name of the active DPOD installation.



```
Installation Environment Name
-----------------------------

Each installation is identified by an environment name.
Separate installations (such as prod/test/dev) must have UNIQUE environment names.
The environment name is also displayed in the Web Console.
Environment names are 4 alphanumeric characters long at most.



Please enter environment name    :>
```

Choose whether you use SSD storage, press "y" to confirm you are using SSD based storage or "n" for non SSD storage.



```
  Storage Optimization
  --------------------

  Storage optimization is required for better system performance, and is based on the data storage
type:
  Solid State Drive (SSD) or traditional spinning hard drive (HDD-SAS)

  To continue with the software installation, the data storage type must be provided.
  You may consult with your system administrator in case the data storage type is unknown.


  Is the data storage type SSD ? [y/n] _
```

When the software update completes, the system will display the following messages on the console output.

```
Starting software update. log file is
/installs/update/fix/logs/montier-update-2017-08-01_16-13-35.log
stopping application ...
application stopped successfully.
starting software update.....
updated complete successfully
starting application ...
application started successfully.
update DPOD-update-1_5_0.sfs was installed successfully. log file
/installs/update/fix/logs/montier-update-2017-08-01_16-13-35.log
```

Please review the upgrade log file if the console displays any error messages.

Upgrade to v1.0.8.0 - Special Steps

DPOD software updates are available from time to time and include enhancements, security updates, component upgrade, bug fixes etc.
The following sections describe the process of upgrading an existing installation.

To upgrade for v.1.0.8.0 you must be at version v1.0.7.0.

You should consider full backup.

Appliance Mode Users Only - The upgrade will upgrade your DPOD installation to an advanced level of Operating System (CentOS 7.4). Therefore the upgrade command will required to be executed twice: 1) For Operating System upgrade 2) For Application upgrade. This procedure will document this to steps upgrade

LDAP files backup - old props files has been backup to a file name

TODO

Obtain the software update

DPOD software updates are available through IBM fix central.

The download consists of two types of files :

1. The update file in the format of : DPOD-fixpack-<version number>.sfs (for example: DPOD-fixpack-1_0_5.sfs)
2. The md5 hash calculation of the update file : DPOD-update-<version number>.md5

Copy the software update to the DPOD server

Copy the update files to the following directory on the DPOD server :

```
/installs/update/fix/TODO
```

If the directory is missing for some reason, please re create it :

```
mkdir -p /installs/update/fix/TODO
```

Install the software update

Run the following command from the location you downloaded the update files to.

```
MonTierUpdateInstaller.sh -u DPOD-update-<version number>.sfs -s
DPOD-update-<version number>.md5
```

For example:

```
MonTierUpdateInstaller.sh -u DPOD-update-1_5_0.sfs -s
DPOD-update-1_5_0.md5
```

After running the command you will be prompted to confirm the software update process. press "Y" to confirm or "N" to abort.

```
Software update :

   Please DO NOT interrupt during the process !

   Are you sure you want to continue ? [y/n]
```

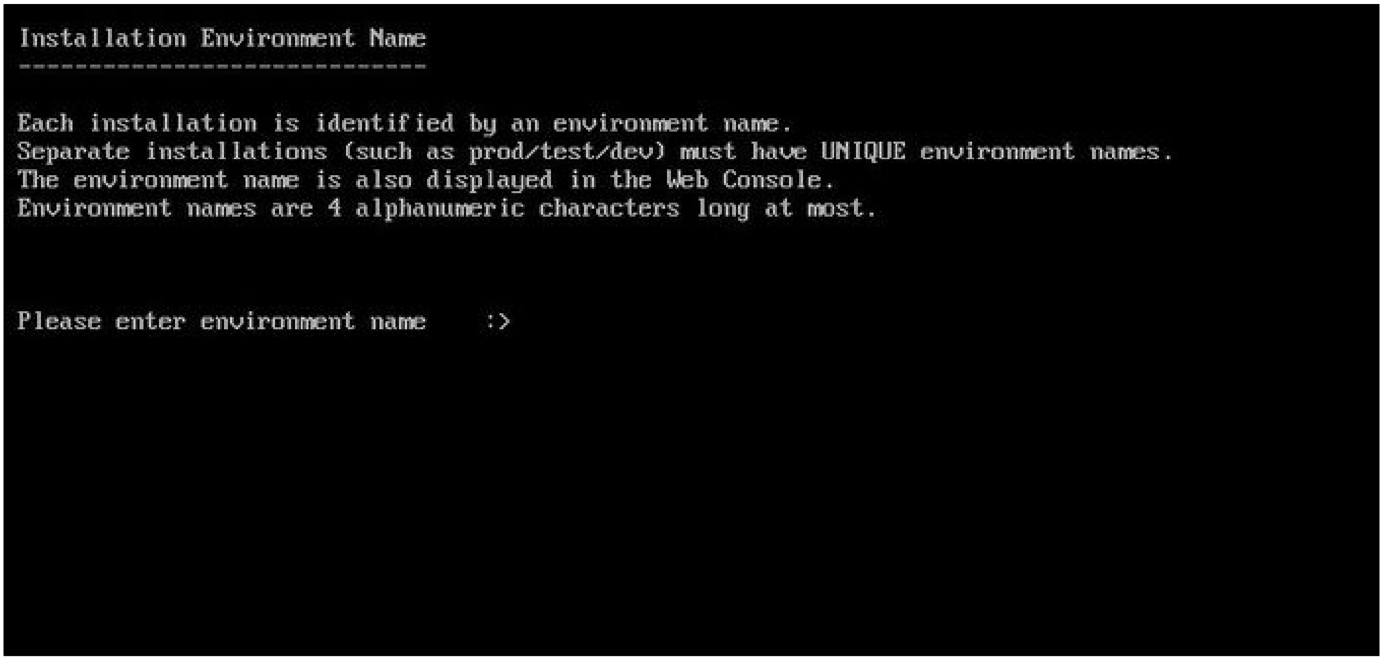
When the software update level is not compatible with the current system version you will receive the following message on the console output :

```
error, software update can NOT be applied to this system version.
aborting update...
```

Do Not interrupt the software update process after it has begun

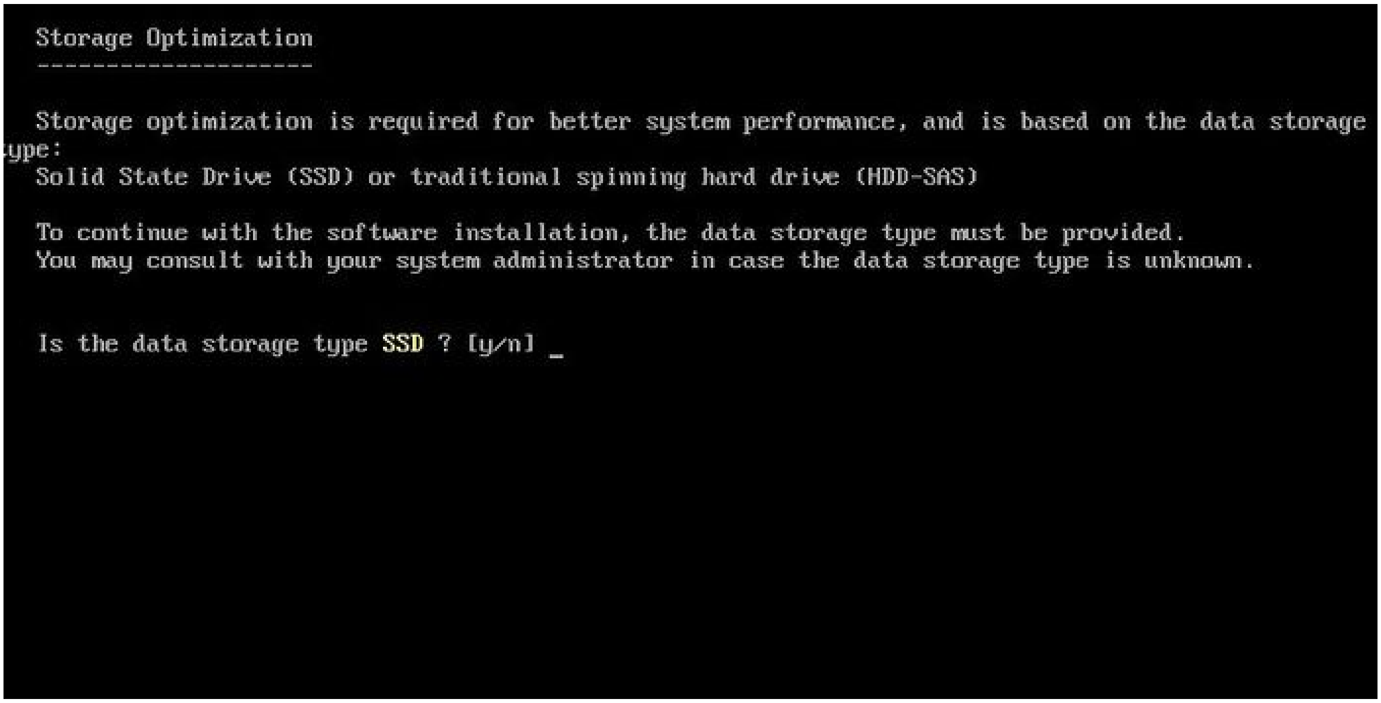
Choose an environment name for this DPOD installation, each DPOD installation must have a **unique** 4-character environment name

If you are installing a second DPOD machine that will be used as the standby machine in a DR Active/Standby scenario, the environment name must be identical to the environment name of the active DPOD installation.



```
Installation Environment Name
-----------------------------

Each installation is identified by an environment name.
Separate installations (such as prod/test/dev) must have UNIQUE environment names.
The environment name is also displayed in the Web Console.
Environment names are 4 alphanumeric characters long at most.



Please enter environment name    :>
```

Choose whether you use SSD storage, press "y" to confirm you are using SSD based storage or "n" for non SSD storage.



```
  Storage Optimization
  --------------------

  Storage optimization is required for better system performance, and is based on the data storage
type:
  Solid State Drive (SSD) or traditional spinning hard drive (HDD-SAS)

  To continue with the software installation, the data storage type must be provided.
  You may consult with your system administrator in case the data storage type is unknown.


  Is the data storage type SSD ? [y/n] _
```

When the software update completes, the system will display the following messages on the console output.

```
Starting software update. log file is
/installs/update/fix/logs/montier-update-2017-08-01_16-13-35.log
stopping application ...
application stopped successfully.
starting software update.....
updated complete successfully
starting application ...
application started successfully.
update DPOD-update-1_5_0.sfs was installed successfully. log file
/installs/update/fix/logs/montier-update-2017-08-01_16-13-35.log
```

Please review the upgrade log file if the console displays any error messages.

Upgrade to v1.0.9.0 - Special Steps

DPOD software updates are available from time to time and include enhancements, security updates, component upgrade, bug fixes etc. The following sections describe the process of upgrading an existing installation.

To upgrade for v.1.0.9.0 you must be at version v1.0.8.5.

You should consider full backup.

Obtain the software update

DPOD software updates are available through IBM fix central.

The download consists of two types of files :

1. The update file in the format of : DPOD-fixpack-<version number>.sfs (for example: DPOD-fixpack-1_0_9.sfs)
2. The md5 hash calculation of the update file : DPOD-update-<version number>.md5

Copy the software update to the DPOD server

Copy the update files to the following directory on the DPOD server :

```
/installs/update/fix/TODO
```

If the directory is missing for some reason, please re create it :

```
mkdir -p /installs/update/fix/TODO
```

Install the software update

Run the following command from the location you downloaded the update files to.

```
MonTierUpdateInstaller.sh -u DPOD-update-<version number>.sfs -s
DPOD-update-<version number>.md5
```

For example:

```
MonTierUpdateInstaller.sh -u DPOD-update-1_0_9.sfs -s
DPOD-update-1_0_9.md5
```

After running the command you will be prompted to confirm the software update process. press "Y" to confirm or "N" to abort.

```
Software update :

   Please DO NOT interrupt during the process !

   Are you sure you want to continue ? [y/n]
```

When the software update level is not compatible with the current system version you will receive the following message on the console output :

```
error, software update can NOT be applied to this system version.
aborting update...
```

Do Not interrupt the software update process after it has begun

On it's first run , the command will complete with the following message :

```
Starting software update. log file is
/installs/update/fix/logs/montier-update-2019-05-20_15-06-06.log

   Found new version of the software update installer... updating
   Software update installer was updated successfully.

   Important !!! Please run the software update installer again.
```

Rerun the upgrade command :

```
MonTierUpdateInstaller.sh -u DPOD-update-1_0_9.sfs -s
DPOD-update-1_0_9.md5
```

Data Migration Tool

The upgrade process checks the existence of Store indices that were created in early versions of the product.
In case that early version indices exist, the upgrade process will stop and notify you of a manual step that you will need to run :

```
Some of the stored application data cannot be migrated to the latest
version of the Store service.

A data migration tool has been deployed in
/installs/data-migration-tool.

You may run it using the following command:

/installs/data-migration-tool/data-migration-tool.sh

Further information can be found in the documentation at:

Admin Guide -> Installation and Upgrade -> Upgrade -> Upgrade to
v1.0.9.0 - Special Steps
```

Configuring the Data Migration Tool

You may edit the configuration file /installs/data-migration-tool/data-migration-tool.conf before running the tool. There are two entries of interest:

- duration.limit (default: 999999) - limits the execution time in minutes.
  This option is useful if you want to schedule the tool to run during off-peak time. In such a case, you can limit the tool to run for a few hours each time and schedule it to start when off-peak time starts, so performance will not be impacted during peak time hours.
- delete.kibana_indices (default: true) - determined whether Kibana indices should be deleted or not.
  true - delete old Kibana indices - all exiting Kibana dashboards and other settings will be deleted.
  false - keep and migrate Kibana indices to the new store version - however Kibana version that comes with DPOD 1.0.9.0 is unable to read the old indices format, so it is up to you to fix the indices manually according to Kibana's documentation.
- Leave the other settings in data-migration-tool.conf as they are, unless advised otherwise by support.

Running the Data Migration Tool

To run the data migration tool manually:

```
/installs/data-migration-tool/data-migration-tool.sh
```

Make sure not to interrupt SSH session during the Data-Migration operation.
Alternatively, you can run the tool in a "no hang-up" mode, which will cause the process to continue running even after the SSH session is closed.
In this mode, the console output will be written to the nohup.log file in the local directory.

```
nohup /installs/data-migration-tool/data-migration-tool.sh &
```

The data migration process may take anywhere between a few minutes and a few days, depending on the amount of data, the server load and the server hardware.
A rough estimation of the time left will be calculated and presented on the console output during the process run. These estimations will also be written to the log file.
The estimation is based on current server load, so it may change significantly between peak and off-peak hours.

Please review the data migration tool log file if the console displays any error message.
When the data migration completes, the console or log file will display the following message:

```
Data migration tool finished successfully
```

Interrupting the Data Migration Tool

Pressing Ctrl+C or setting duration.limit in the configuration file will stop the tool during the migration process.
Stopping the tool will cause it to re-process the last index that was migrated on the next run.

While this is usually not an issue, note that on some cases it may cause complications, for example:
1. The user wants the tool to run during a nightly maintenance window, between 2-4 AM.
2. The tool is scheduled using cron to 2 AM and the duration.limit setting is set to 120 minutes.
3. For this specific user, depending on its hardware and data sizes, processing of each index takes about 3 hours.
4. Since the tool is interrupted after 2 hours, on the next night, the tool will try to migrate the same index again and will never advance to the next index.

Resuming Software Update

To proceed with the software update, you can rerun the software update command:

```
MonTierUpdateInstaller.sh -u DPOD-update-1_0_9.sfs -s
DPOD-update-1_0_9.md5
```

When the software update completes, the system will display the following messages on the console output.

```
Starting software update. log file is
/installs/update/fix/logs/montier-update-2019-05-20_15-07-06.log
2019-05-20_15-07-17: INFO Starting software update (JRE). log file is
/installs/update/fix/logs/montier-update-2019-05-20_15-07-06.log
2019-05-20_15-07-51: INFO Stopping application ...
2019-05-20_15-08-47: INFO Application stopped successfully.
2019-05-20_15-09-29: INFO Starting software update (JRE).
2019-05-20_15-10-33: INFO Starting software update (1.0.9.0). log file
is /installs/update/fix/logs/montier-update-2019-05-20_15-07-06.log
2019-05-20_15-10-37: INFO Stopping application ...
2019-05-20_15-11-27: INFO Application stopped successfully.
2019-05-20_15-11-28: INFO Starting software update (1.0.9.0).
2019-05-20_15-17-18: INFO Updated complete successfully (1.0.9.0).  log
file /installs/update/fix/logs/montier-update-2019-05-20_15-07-06.log.
2019-05-20_15-17-24: INFO Starting application ...
2019-05-20_15-19-55: INFO Application started successfully.
2019-05-20_15-20-00: INFO Please update store allocation now
2019-05-20_15-20-00: INFO Using the admin console in https://<your
server name>/admin
2019-05-20_15-20-00: INFO Admin Console -> Utilities -> Store -> Store
Allocation
update DPOD-update-1_0_9.sfs was installed successfully. log file
/installs/update/fix/logs/montier-update-2019-05-20_15-07-06.log
```

Please review the upgrade log file if the console displays any error messages.

Update Store Allocation

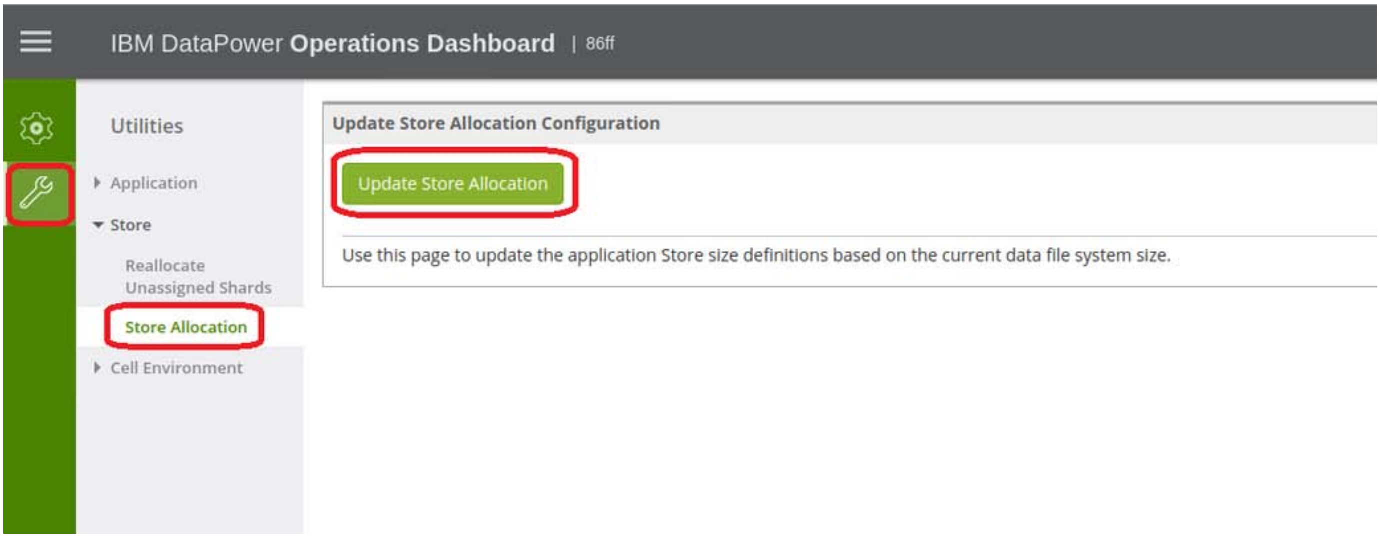
Open the DPOD admin console on your favorite browser:

https://<your server name>/admin

Go to:

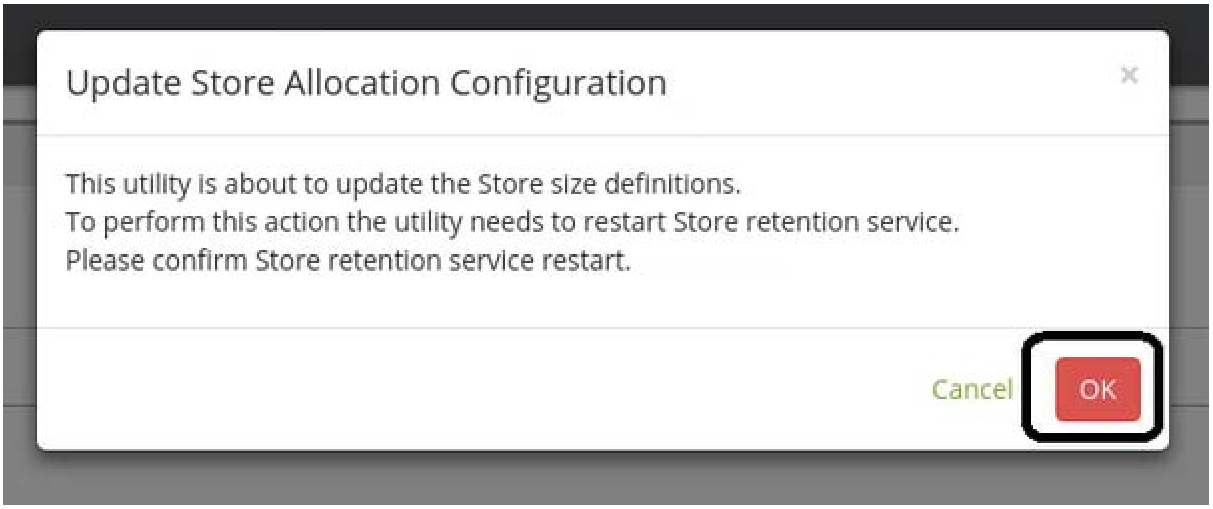
Admin Console -> Utilities -> Store -> Store Allocation

Run the Update Store Allocation utility:


IBM DataPower Operations Dashboard | 86ff
Utilities
Application
Store
Reallocate Unassigned Shards
Store Allocation
Cell Environment
Update Store Allocation Configuration
Update Store Allocation

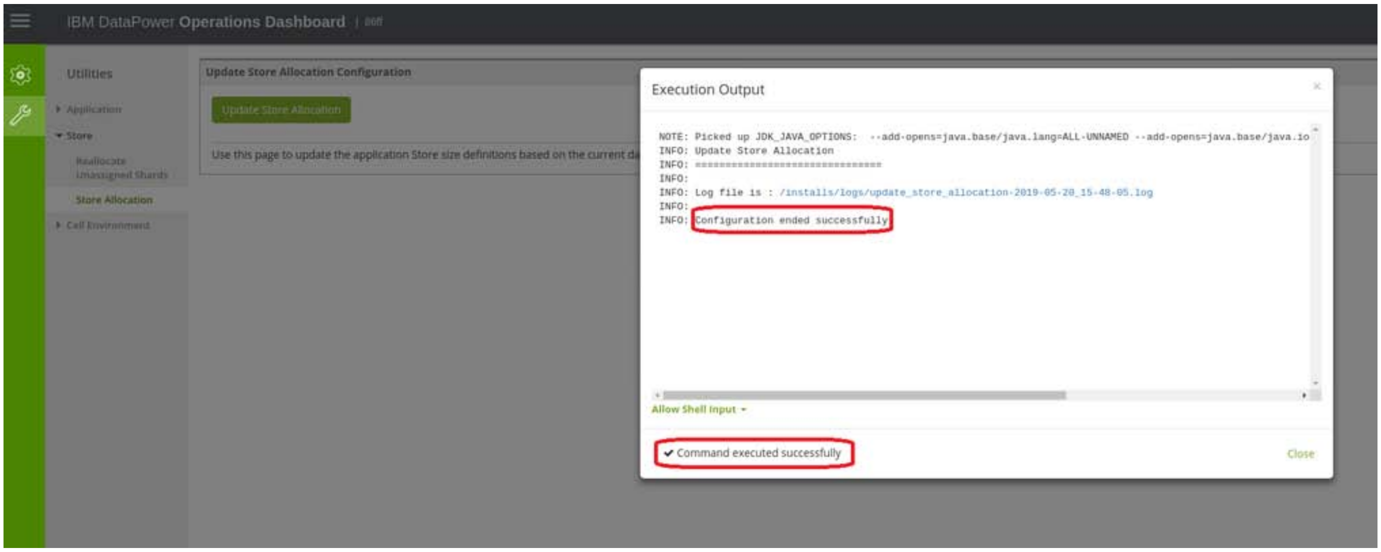
Use this page to update the application Store size definitions based on the current data file system size.

Confirm the operation :



This utility is about to update the Store size definitions.
To perform this action the utility needs to restart Store retention service.
Please confirm Store retention service restart.

The execution output window will appear. Wait for the "Command executed successfully" indication, and check that the line "Configuration ended successfully" in the output.



Update Store Allocation Configuration

Use this page to update the application Store size definitions based on the current da

Execution Output

```
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io
INFO: Update Store Allocation
INFO: ===============================
INFO:
INFO: Log file is : /installs/logs/update_store_allocation-2019-05-20_15-48-05.log
INFO:
INFO: Configuration ended successfully
```

✓ Command executed successfully

Uninstall

DPOD removal includes two main stages :

- Remove DPOD from the DataPower gateways
- Remove DPOD application from the installed server (Appliance mode / Non Appliance mode)

DPOD removal is not applicable for Docker container edition and Developer edition

Remove DPOD From the DataPower Gateways

How to Uninstall DPOD from DataPower

Remove DPOD Application From the Installed Server

In order to remove DPOD application from the installed server (Appliance mode / Non Appliance mode), execute the following commands:

```
cd /
montier_env_uninstall.sh
```

Output example:

```
2017-03-06_12-58-15: montier_environment: Locating the scripts
directory.
2017-03-06_12-58-15: montier_environment: Did not find previous
SCRIPTS_DIR environment variable. Using default : /app/scripts
2017-03-06_12-58-15: montier_environment: Locating the montier_props
file.
2017-03-06_12-58-15: montier_environment: Locating build environment
variables script.
2017-03-06_12-58-15: montier_environment: Building environment variables
file.
2017-03-06_12-58-17: montier_environment: Obtaining environment
variables.
2017-03-06_12-58-17: montier_environment: Stopping MonTier services.
Stopping MonTier:

2017-03-06_12-58-56: montier_environment: Setting the packages to
uninstall.
2017-03-06_12-58-56: montier_environment: Reading the user uninstall
packages choices.
2017-03-06_12-58-56: montier_environment: Uninstalling products.
2017-03-06_12-59-09: montier_environment: Removing Balancer package.
2017-03-06_12-59-10: montier_environment: Removing Logical-Trans
package.
2017-03-06_12-59-11: montier_environment: Removing WSM package.
2017-03-06_12-59-12: montier_environment: Removing Syslog package.
2017-03-06_12-59-13: montier_environment: Removing Console package.
2017-03-06_12-59-14: montier_environment: Removing Big-Data package.
2017-03-06_12-59-15: montier_environment: Removing Base package.
2017-03-06_12-59-16: montier_environment: Removing montier_props
environment variable from the application users bashrc files.
2017-03-06_12-59-16: montier_environment: Removing
packages_to_install.sh and packages_to_uninstall.sh files.
2017-03-06_12-59-16: montier_environment: Removing installation_base.sh
file.
2017-03-06_12-59-16: montier_environment: Saving current arch.properties
file to
/installs/arch.properties/previous.arch.properties.2017-03-06_12-59-16.
2017-03-06_12-59-16: montier_environment: Removing environment RPM.
2017-03-06_12-59-16: montier_environment: Removing MonTier left-over
processes.
2017-03-06_12-59-16: montier_environment: Removing MonTier left-over
hosts from /etc/hosts.
--------------------
2017-03-06_12-59-17: montier_environment ended successfully.
Please verify all procedures executed correctly.
Log file:
/installs/logs/montier_environment_uninstallation_2017-03-06_12-58-15.lo
g
```

- How to Uninstall DPOD from DataPower

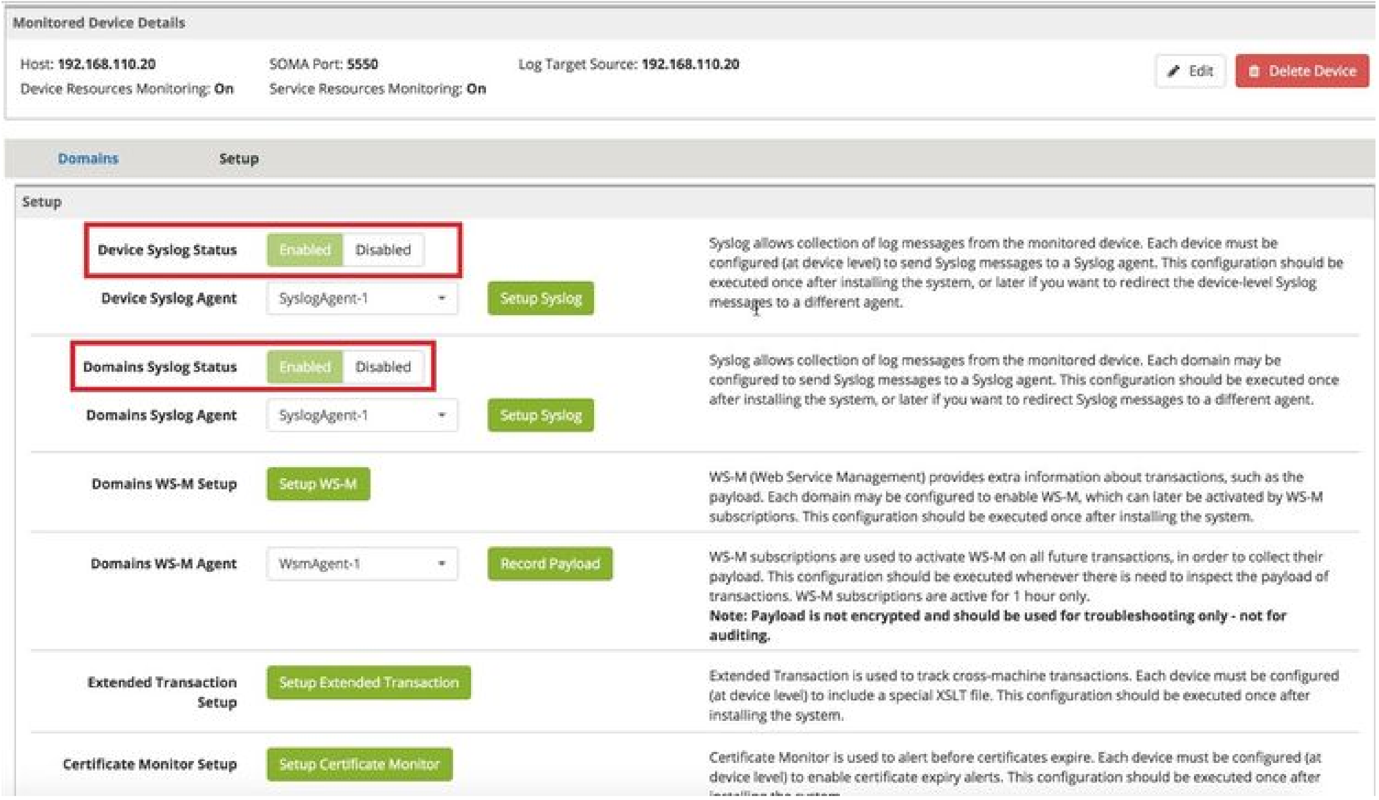
How to Uninstall DPOD from DataPower

DPOD was designed to be non-intrusive. Therefore, there are only a few steps required to reverse its setup on the DataPower device.

> This page describe how to manually remove DPOD's configuration from a monitored device. Alternatively, you can run a script to automatically remove the setup. See Backing up and Restoring DPODs IDG related configuration

Before you Start

You do not need to uninstall DPOD if you only need to disable it for investigation purposes.
You can stop DataPower from sending syslogs to DPDD by selecting "Monitored Devices" from the Manage menu, and changing the "Device Syslog Status" to disabled.



Monitored Device Details

Host: **192.168.110.20**
Device Resources Monitoring: **On**
SOMA Port: **5550**
Service Resources Monitoring: **On**
Log Target Source: **192.168.110.20**

Setup

Device Syslog Status: Enabled | Disabled

Device Syslog Agent: SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each device must be configured (at device level) to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect the device-level Syslog messages to a different agent.

Domains Syslog Status: Enabled | Disabled

Domains Syslog Agent: SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect Syslog messages to a different agent.

Domains WS-M Setup

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration should be executed once after installing the system.

Domains WS-M Agent: WsmAgent-1

WS-M subscriptions are used to activate WS-M on all future transactions, in order to collect their payload. This configuration should be executed whenever there is need to inspect the payload of transactions. WS-M subscriptions are active for 1 hour only.
Note: Payload is not encrypted and should be used for troubleshooting only - not for auditing.

Extended Transaction Setup

Extended Transaction is used to track cross-machine transactions. Each device must be configured (at device level) to include a special XSLT file. This configuration should be executed once after installing the system.

Certificate Monitor Setup

Certificate Monitor is used to alert before certificates expire. Each device must be configured (at device level) to enable certificate expiry alerts. This configuration should be executed once after installing the system.

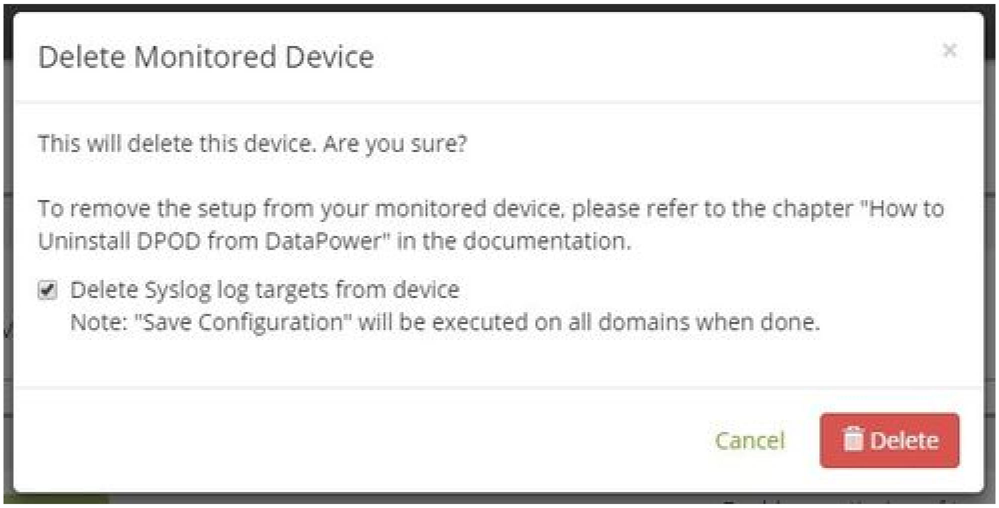
To uninstall DPOD, perform the following steps on your monitored DataPower device.

These steps can be done **manually** as describe below or a by **using scripts** as described in Backing up and Restoring DPODs IDG related configuration

Remove Syslog Targets

You can remove DPOD's log targets from the monitored device automatically or manually:

1. Automatically - from DPOD's ManageDevices->Monitored Devices page, select the monitored device and click "Delete Device", check the box "Delete Syslog log targets from device" in the confirmation window.



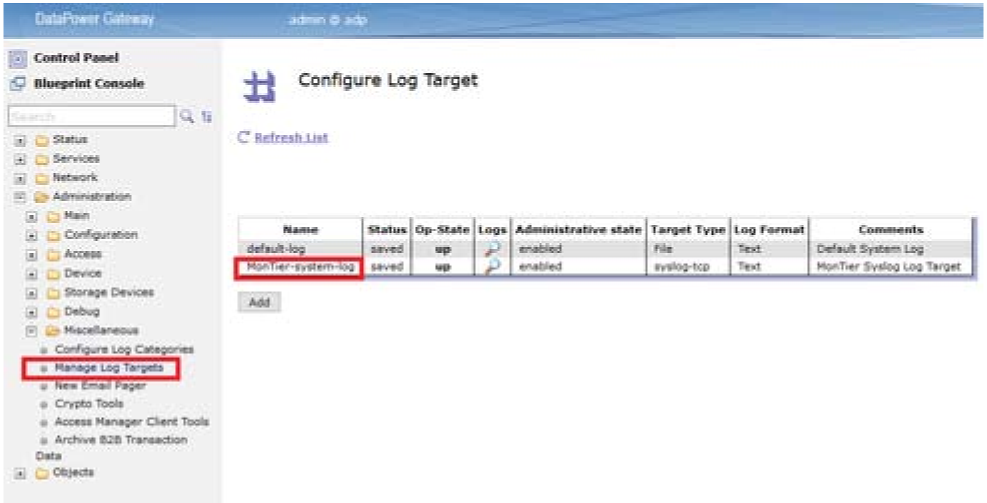
Delete Monitored Device

This will delete this device. Are you sure?

To remove the setup from your monitored device, please refer to the chapter "How to Uninstall DPOD from DataPower" in the documentation.

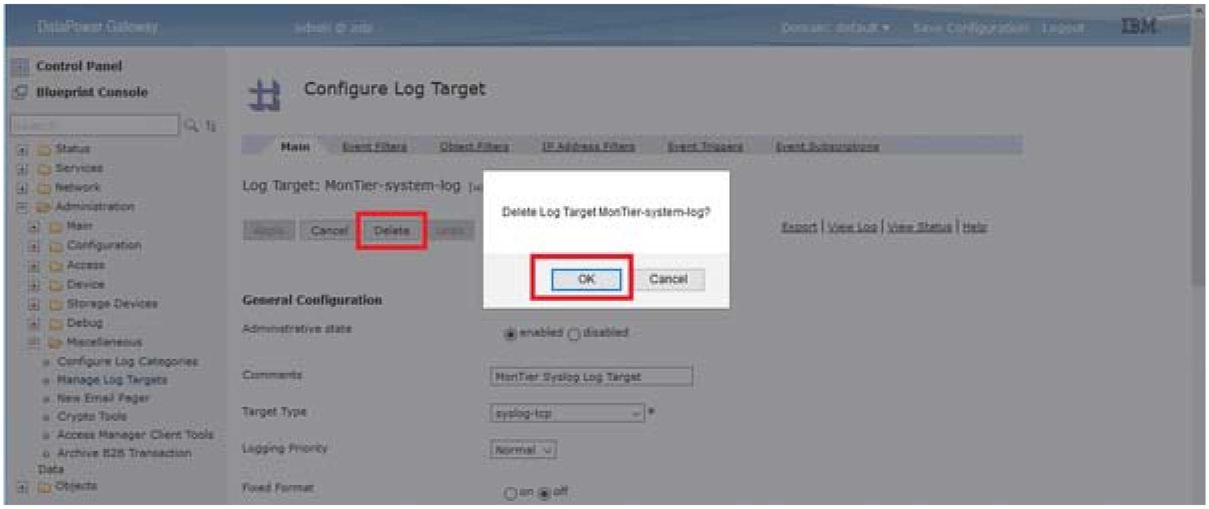
☑ Delete Syslog log targets from device
Note: "Save Configuration" will be executed on all domains when done.

2. Manually - On the Gateway's “Manage Log Targets” screen, select all log targets starting with “Montier*” and "DPOD-MSC*" and delete them.



Configure Log Target

Name	Status	Op-State	Logs	Administrative state	Target Type	Log Format	Comments
default-log	saved	up	🔍	enabled	File	Text	Default System Log
MonTier-system-log	saved	up	🔍	enabled	syslog-tcp	Text	MonTier Syslog Log Target



Configure Log Target

Log Target: MonTier-system-log

Delete Log Target MonTier-system-log?

General Configuration

Administrative state ● enabled ○ disabled

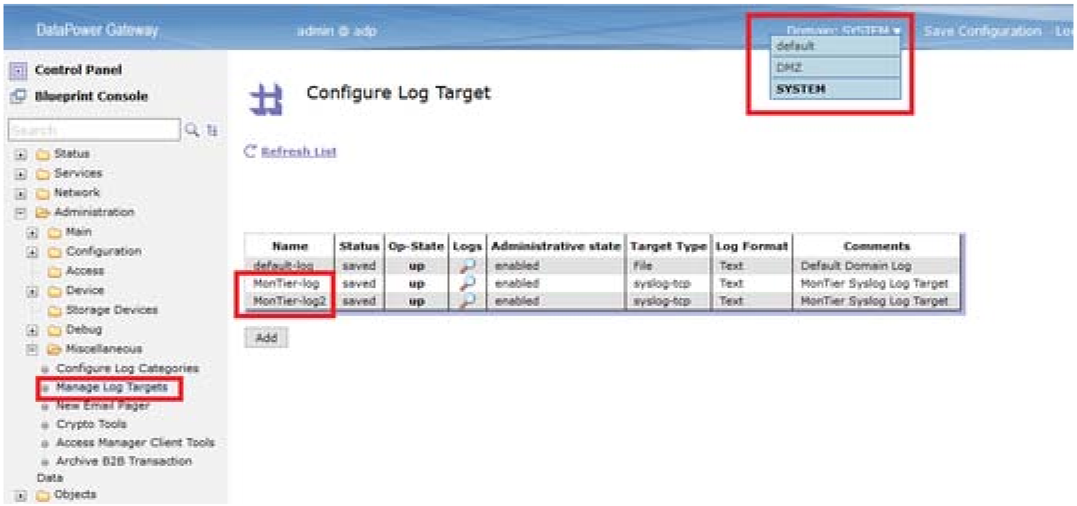
Comments: MonTier Syslog Log Target

Target Type: syslog-tcp *

Logging Priority: Normal

Fixed Format ○ on ● off

Repeat for all domains:

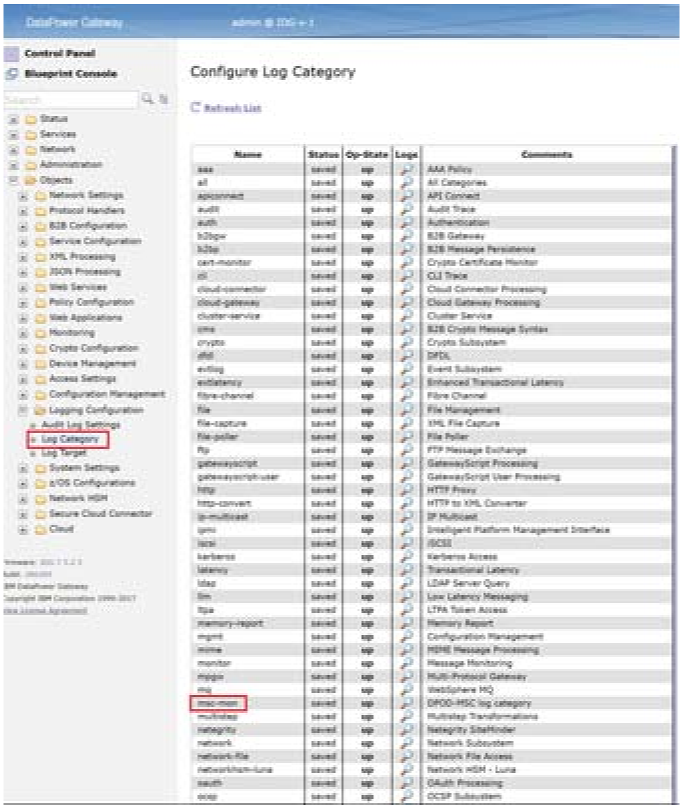


Configure Log Target

Name	Status	Op-State	Logs	Administrative state	Target Type	Log Format	Comments
default-log	saved	up	🔍	enabled	File	Text	Default Domain Log
MonTier-log	saved	up	🔍	enabled	syslog-tcp	Text	MonTier Syslog Log Target
MonTier-log2	saved	up	🔍	enabled	syslog-tcp	Text	MonTier Syslog Log Target

Remove Log Categories

On the "Log Categories" screen, delete all the categories starting with "montier" or "msc-"

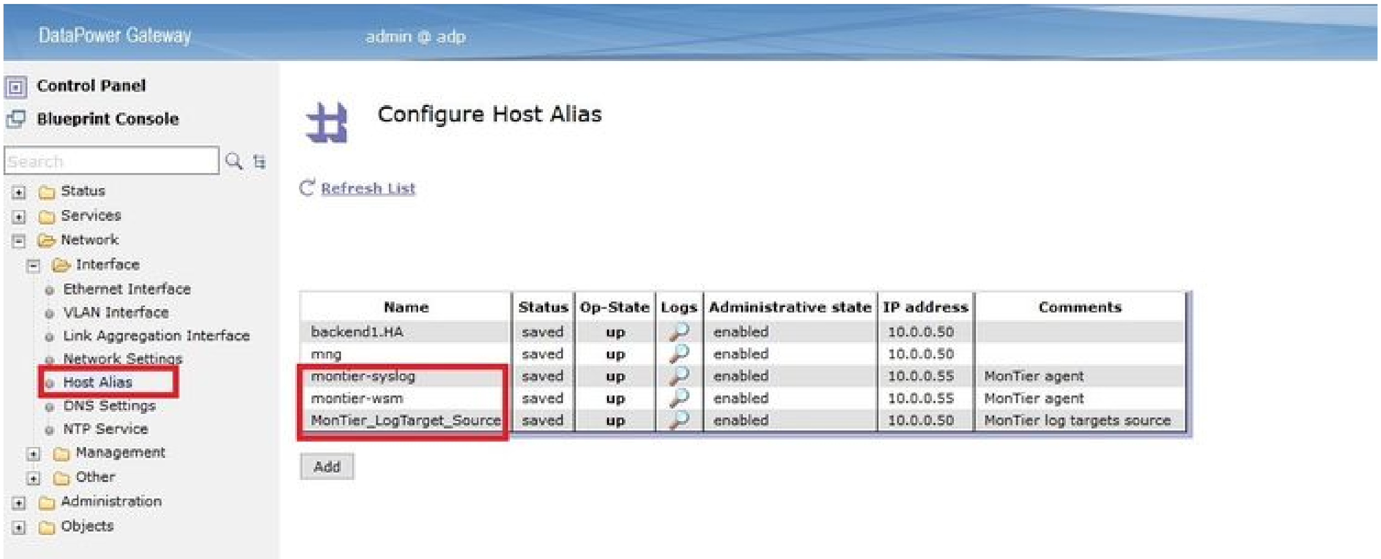


Configure Log Category

Name	Status	Op-State	Logs	Comments
aaa	saved	up	🔍	AAA Policy
all	saved	up	🔍	All Categories
apiconnect	saved	up	🔍	API Connect
audit	saved	up	🔍	Audit Trace
auth	saved	up	🔍	Authentication
b2bgw	saved	up	🔍	B2B Gateway
b2bp	saved	up	🔍	B2B Message Persistence
cert-monitor	saved	up	🔍	Crypto Certificate Monitor
cli	saved	up	🔍	CLI Trace
cloud-connector	saved	up	🔍	Cloud Connector Processing
cloud-gateway	saved	up	🔍	Cloud Gateway Processing
cluster-service	saved	up	🔍	Cluster Service
cms	saved	up	🔍	B2B Crypto Message Syntax
crypto	saved	up	🔍	Crypto Subsystem
dfdl	saved	up	🔍	DFDL
evtlog	saved	up	🔍	Event Subsystem
extlatency	saved	up	🔍	Enhanced Transactional Latency
fibre-channel	saved	up	🔍	Fibre Channel
file	saved	up	🔍	File Management
file-capture	saved	up	🔍	XML File Capture
file-poller	saved	up	🔍	File Poller
ftp	saved	up	🔍	FTP Message Exchange
gatewayscript	saved	up	🔍	GatewayScript Processing
gatewayscript-user	saved	up	🔍	GatewayScript User Processing
http	saved	up	🔍	HTTP Proxy
http-convert	saved	up	🔍	HTTP to XML Converter
ip-multicast	saved	up	🔍	IP Multicast
ipmi	saved	up	🔍	Intelligent Platform Management Interface
iscsi	saved	up	🔍	iSCSI
kerberos	saved	up	🔍	Kerberos Access
latency	saved	up	🔍	Transactional Latency
ldap	saved	up	🔍	LDAP Server Query
llm	saved	up	🔍	Low Latency Messaging
ltpa	saved	up	🔍	LTPA Token Access
memory-report	saved	up	🔍	Memory Report
mgmt	saved	up	🔍	Configuration Management
mime	saved	up	🔍	MIME Message Processing
monitor	saved	up	🔍	Message Monitoring
mpgw	saved	up	🔍	Multi-Protocol Gateway
mq	saved	up	🔍	WebSphere MQ
msc-mon	saved	up	🔍	DPOD-MSC log category
multistep	saved	up	🔍	Multistep Transformations
netegrity	saved	up	🔍	Netegrity SiteMinder
network	saved	up	🔍	Network Subsystem
network-file	saved	up	🔍	Network File Access
networkhsm-luna	saved	up	🔍	Network HSM - Luna
oauth	saved	up	🔍	OAuth Processing
ocsp	saved	up	🔍	OCSP Subsystem

Remove Host Aliases

On the "Host Aliases" screen, delete all the aliases starting with "montier" or "MSC-"



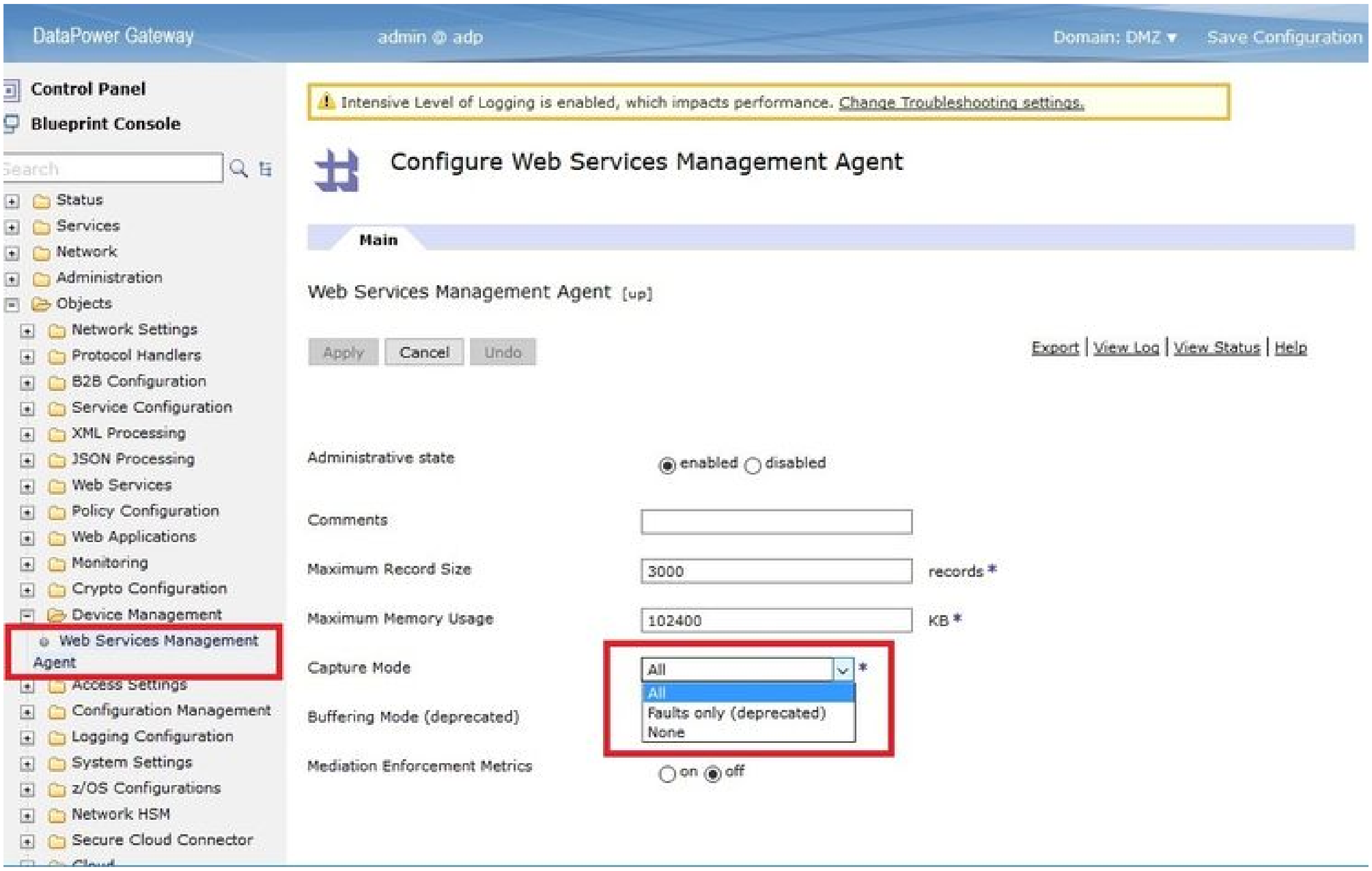
Configure Host Alias

Name	Status	Op-State	Logs	Administrative state	IP address	Comments
backend1.HA	saved	up	🔍	enabled	10.0.0.50	
mng	saved	up	🔍	enabled	10.0.0.50	
montier-syslog	saved	up	🔍	enabled	10.0.0.55	MonTier agent
montier-wsm	saved	up	🔍	enabled	10.0.0.55	MonTier agent
MonTier_LogTarget_Source	saved	up	🔍	enabled	10.0.0.50	MonTier log targets source

(Optional) Change Web Services Management Capture Mode

> Do not perform this step if you have WS-M Agent Subscribers other than DPOD, as they will stop working too.

On the “Web Services Management Agent” screen, change "Capture Mode" from “All” to “None” or “Faults only”



⚠ Intensive Level of Logging is enabled, which impacts performance. Change Troubleshooting settings.

Configure Web Services Management Agent

Web Services Management Agent [up]

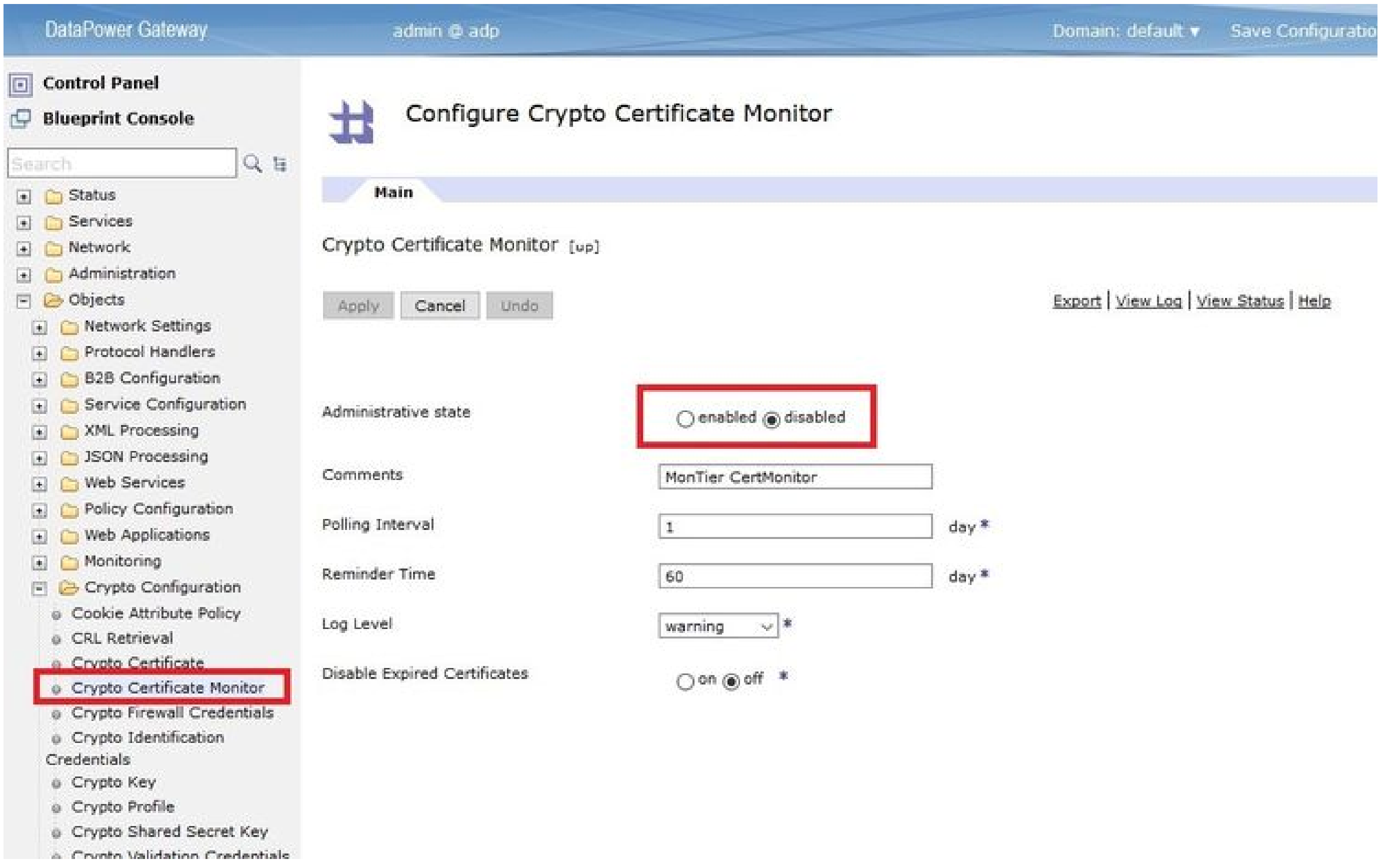
Administrative state	● enabled ○ disabled
Comments	
Maximum Record Size	3000 records *
Maximum Memory Usage	102400 KB *
Capture Mode	All * (All / Faults only (deprecated) / None)
Buffering Mode (deprecated)	
Mediation Enforcement Metrics	○ on ● off

(Optional) Disable the Certificate Monitor

> The certificate monitor writes a syslog record for each expired certificate.
> Leaving it as is will not have much effect (except for writing a few syslog records from time to time). As its impact is low - this step may

> be skipped unless there is a specific reason to disable it.

On the “Crypto Certificate Monitor” screen, change the Administrative state to “disabled”



Configure Crypto Certificate Monitor

Crypto Certificate Monitor [up]

Administrative state	○ enabled ● disabled	
Comments	MonTier CertMonitor	
Polling Interval	1	day *
Reminder Time	60	day *
Log Level	warning	*
Disable Expired Certificates	○ on ● off	*

(Optional) XSLT

> Leaving the policies as they are and skipping this step will have no effect on the service(s)

In every webservice proxy, go into the processing policy and remove the Montier policy from all the processing rules

Verify all the objects in this list are removed

Objects to remove

Decommission the DPOD machine

When all steps above are completed, the DPOD appliance may be decommissioned safely.

Management and Configuration

DPOD provides several methods for administrators to perform management and configuration tasks such as starting and stopping services, or checking their status.

The following sections describe the various management methods in detail.

- Manage using the Web console
- Using the Command Line Interface (CLI)
- System Services Management
- Common Administration Tasks
- System Directories structure

Manage using the Web console

DPOD provides an easy to use Graphical User Interface. The interface lets administrators perform system administration tasks in a familiar, browser-based environment.

DPOD's management options are accessible to users with administrative privileges via the The Navigation Bar, by clicking on the ⚙ icon.

> All UI components described in this section comply with the concept presented at Web Console.

The following sections describe management tasks accessible through the UI.

- Device Management
- Customize
- Security Management
- System Management
- Transactions
- Internal Health

.

Device Management

The Devices section under **[ManageDevices]** provides access to the set of devices monitored by DPOD.

> This step changes or add some of you monitored device objects. Please review the list of changes before you continue too perform this actions.

Monitored Devices

This screen displays a table containing information on all the monitored devices connected to DPOD's console, and lets an administrator perform several configuration tasks, at a device, domain or service level.
Each row in the table contains the following details about a single device:

Column	Description
Name	The device's name in DPOD
Host	IP Address of the device
SOMA port	The SOMA port configured on this device
Log Target Source	IP Address of the device's log target source
Device Resources Monitoring	Whether Device resources monitoring is enabled on this device
Service Resources Monitoring	Whether Service resources monitoring is enabled on this device

(This information relates to the information entered when Adding Monitored Devices)

Device Level Configuration

The following steps let an administrator perform device-level configuration tasks:

1. Click on one of the monitored devices in the Monitored Devices table.
   The system displays the device details, and a list of all the domains on that device.
2. Click the **Setup** link (found at the top of the table, next to the label 'Domains')
   The system displays a list of administrator tasks available for this device. Consult the tables at the end of this page to find details about the available tasks.

Domain Level Configuration

The following steps let an administrator perform domain-level configuration tasks:

1. Click on one of the monitored devices in the Monitored Devices table.
   The system displays the device details, and a list of all the domains on that device.
2. Click on one of the domains to select it.
   The system displays the domain's details and a list of all services running on the selected domain.
3. Click the **Setup** link (found at the top of the table, next to the label 'Services')
   The system displays a list of administrator tasks available for this domain. Consult the tables at the end of this page to find details about the available tasks.

Service Level Configuration

The following steps let an administrator perform service-level configuration tasks:

1. Click on one of the monitored devices in the Monitored Devices table.
   The system displays the device details, and a list of all the domains on that device.
2. Click on one of the domains to select it.
   The system displays the domain's details and a list of all services running on the selected domain.
3. Click on one of the services.
   The system displays the service's details and a list of all endpoints in the service
4. Click the **Setup** link (found at the top of the table, next to the label 'Endpoints')
   The system displays a list of administrator tasks available for this service. Consult the tables at the end of this page to find details about the available tasks.

This step changes or adds some of your monitored device objects. Please review the list of changes before you continue too perform this actions.

Available Tasks (Operations)

Device Level Operation Details

The following tasks are available for devices setup.

If you wish to monitor transactions in the default domain, please follow the instructions in this page.

Task (Operation)	Details
Setup Syslog for device	Sets up the necessary configuration for the device to send device-level Syslog records to the selected agent. This configuration should be executed once after installing the system or when you need to redirect the device-level Syslog messages to a different agent. To setup the Syslog for a device, select a Syslog Agent from the drop-down list, and click the **Setup Syslog for device** button. You can disable/enable this Syslog target by clicking on the "Device Syslog Status" Enabled/Disabled buttons. **Limitation**: DPOD does not support transactions in the default domain. See limitation section. **Note: This action changes your device configuration - please review changes .**
Setup Syslog for all domains	Sets up the necessary configuration for all the domains to send domain-level Syslog records to the selected agent. This configuration should be executed once after installing the system, when a new domain is created or when you need to redirect the device-level Syslog messages to a different agent. To setup the log targets for all domains, select a Syslog Agent from the drop-down list, select analysis level from the drop-down list, and click the **Setup Syslog** button. You can disable/enable all log targets by clicking on the "Domains Syslog Status" Enabled/Disabled buttons. **Limitation**: DPOD does not support more than 125 domains per device. See limitation section . Trying to run this action on more than 125 domains can be unpredictable. If you have more than 125 domains, you **MUST** run "Setup Syslog" using the Domain Level procedure below. **Note: This action changes your device configuration - please review changes .**
Auto Setup Domains	This feature will automatically detect and setup new domains created on the monitored device, this is especially useful for dynamically created API Connect domains. Choose a Syslog agent and a WS-M agent that the domains should report to, select analysis level from the drop-down list, enter the domain pattern (use asterisk as wildcard) and click save. DPOD will scan the monitored device every 2 minutes and will setup the new domain (you can change the interval from the system parameters page. A UI service restart is required after changing this interval)
Setup WS-M for all domains	Sets up the necessary configuration for all the domains to send payload data to the selected agent This configuration should be executed once after installing the system, when a new domain is created or when you need to redirect the payloads to a different agent Clicking the "Record Payload" link will take you to the Payload Capture page, where you can start a WS-M subscription. **Note: This action changes your device configuration - please review changes .** **Note:** This action does not enable the WS-M Agent on IDG. For security reasons, this can only be done from IDG.
Setup Certificate Monitor for device	The Certificate Monitor is used to provide alerts before certificate expiration. Each device must be configured (at the device level) to enable certificate expiry alerts. This configuration should be executed once after installing the system. **Note: This action changes your device configuration - please review changes .**

Setup Extended Transactions for device	**This option was deprecated and was replaced by a non-intrusive method, please do not use it unless advised by L2/L3 support.** Extended Transactions are used to track cross-machine transactions, i.e. messages which are forwarded from one monitored DataPower Gateway to another. To use Extended Transactions, the devices must be configured (at device level). Extended transactions can be configured through the Web Console. **Note: This action changes your device configuration - please review changes .**

This step changes some of your monitored device objects. Please review the list of changes before you continue with this action.

Domain Level Operation Details

The following tasks are available for domains setup.

Task (Operation)	Details
Setup Syslog	Sets up the necessary configuration for this domain to send domain-level Syslog records to the selected agent. This configuration should be executed once after installing the system, or when the domain-level Syslog messages need to be redirected to a different agent. To setup the Syslog for a domain, select a Syslog Agent from the drop-down list, and click the **Setup Syslog** button. You can disable/enable this Syslog target by clicking on the "Domain Syslog Status" Enabled/Disabled buttons. **Note: This action changes your device configuration - please review changes .**
Setup WS-M	Sets up the necessary configuration for all the domains to send payload data to the selected agent. This configuration should be executed once after installing the system, when a new domain is created or when the payloads need to be redirected to a different agent. Clicking the "Record Payload" link will take you to the Payload Capture page, where you can start a WS-M subscription. **Note: This action changes your device configuration - please review changes .** **Note:** This action does not enable the WS-M Agent on IDG. This can be done only from IDG for security reasons.
Setup Extended Transactions for all services	**This option was deprecated and was replaced by a non-intrusive method, please do not use it unless advised by L2/L3 support.** Extended Transactions are used to track cross-machine transactions, i.e. messages which are forwarded from one monitored DataPower Gateway to another. Choosing this option will enable support for extended transactions for services on this domain. This is performed by adding a new step to all the services, which inserts the Extended Transaction correlation ID into the message header. DPOD uses this correlation ID to track the extended transactions. This configuration should be executed once after installing the system (either at a service or a domain level), or when you need to add extended transaction support for services in the domain. If extended transactions were previously enabled for some of the services in this domain, executing this will add the new step to new services only - the previously configured services will be unaffected. **Note: This action is intrusive and changes your service configuration and may require manual rollback - please review changes .**

This step changes some of your monitored device objects. Please review the list of changes before you continue with this action.

Service Level Operation Details

The following task is available for services setup.

Task (Operation)	Details

Setup Extended Transactions	**This option was deprecated and was replaced by a non-intrusive method, please do not use it unless advised by L2/L3 support.** Extended Transactions are used to track cross-machine transactions, i.e. messages which are forwarded from one monitored DataPower Gateway to another. Choosing this option will enable support for extended transactions for the service. This is performed by adding a new step to the service, which inserts the Extended Transaction correlation ID into the message header. DPOD uses this correlation ID to track the extended transactions. This configuration should be executed once after installing the system (either at a service or a domain level), or when you need to add extended transaction support for services in the domain. Executing this again for a service that has already been enabled for extended transactions will not change its state. **Note: This action is intrusive and changes your service configuration and may require manual rollback - please review changes .**

DEVICE HEALTH SETTINGS

- For each device, the user can define whether the device is displayed in the System Health dashboard, Damage Points Threshold, Total Warnings Threshold
    - **Damage Points Threshold** - number of damage points that defines the device to be in an **Error** state
    - **Total Warnings Threshold** - total warnings that defines the device to be in an **Error** state
- For each device, the user can set thresholds and damage points per health metric.
    - Thresholds can be set only for metrics that support thresholds (such as Frequency or Flat-Line).

DEVICES GROUPS

The screen is accessible by clicking **[ManageDevicesDevices Groups]** from the The Navigation Bar.

Devices Groups Table

All the devices groups defined in the system are listed in a table. Each row in the table contains the following information for a single group:

Column	Description
Name	The group's name. Clicking on a group's name will load the group's details in the Group View and provide access to system actions for the group.
Description	The description for this group

Adding a Devices Group

The devices groups table screen contains the **Add Group** button at the top.
Click this button to add a new group in the system.

You will need to set the group's name and description.

Reordering Devices Groups

Each row in the table contains the **Move Up** button which allows reordering of the groups, for example this will effect the order in which the groups are displayed in the System Health dashboard.

Devices Group View

The devices group view is loaded for a device group when the device's group name is clicked from the Groups Table described above.

The system displays the following details:

Detail	Content Description
Name	The devices group's name
Description	A description attached to this devices group
Devices in Group	This widget lists all Devices in this group. You may use the controls in this widget to remove/move up devices from the group or add new devices to it. Clicking a device will open the Monitored Device View for the selected device

Edit or Delete a Device's Group

The Devices Group View screen contains two buttons at the top.

Click the **Edit** button to edit the displayed devices group's details. You may alter the devices group's name and description.

Click the **Delete Group** button to remove the devices group from the system.

LOG TARGET ANALYSIS LEVELS

The Log Target Analysis Level determines how many syslogs will be sent from the monitored device to DPOD.

Each analysis level is composed of message groups that allow DPOD to show information about the transactions (see the message groups descriptions below)
In addition, each analysis level will only show syslog messages that are equal or above a certain log level.

The Default analysis level for IDG domains is Max Data
The Default analysis level for API Connect domains is Balanced + SideCalls

Analysis Level Name	Message Groups	Log Level
Max Data	Core, MemoryReqRes, B2B, MemActionLevel, ReqPayloadSize, ExtLatency, Sidecalls	info
More Data	Core, MemoryReqRes, B2B, MemActionLevel, ReqPayloadSize, ExtLatency	info
Balanced	Core, MemoryReqRes, B2B, MemActionLevel	notice
More TPS	Core, MemoryReqRes, B2B	notice
Max TPS	Core, MemoryReqRes, B2B	error

Message Group Name	Description
Core	Required, DPOD may not show any data without this message group
MemoryReqRes	Required, DPOD may not show any data without this message group
B2B	This message group will enable special B2B filters in the Raw Messages page (like "B2B Message ID" and "B2B From Partner ID"), DPOD will show B2B transactions even without this message group
MemActionLevel	This message group will populate the memory graph in the transaction page, DPOD will show basic memory data even without this message group
ReqPayloadSize	This message group will populate service request size information in some dashboards, such as the Recent Activity dashboard
ExtLatency	This message group will populate the transaction's extended latency tab in the transaction page.
SideCalls	This message group will populate the sidecalls tab in the transaction page

Customize Analysis Levels

You can configure which message groups and log level are assigned to each analysis level from the system parameters (For example, the parameters "Transaction Analysis Level - Balanced" will assign message groups and log level to the Balanced analysis level)
In most cases, you can leave the default analysis levels setup

Customize Message Groups

If you wish to add or remove specific syslog messages from a message group, you can specify an override file, specify the file's location in the system parameter "Transaction Analysis Level - User Override Path"

The file should contain one or more lines to add or remove messages to message groups,
To add messages to a message group use:
+.messageGropName.syslogMessageCode=logLevel.logCategory,logLevel.logCategory,logLevel.logCategory

For Example
+.MemActionLevel.0x80e0013f=debug.memory-report
Will add the message 0x80e0013f (debug log level and above, with log category memory-report) to the message group MemActionLevel

+.B2B.0x80123456=debug.b2bgw, error.mpgw
Will add the message 0x80123456 (debug log level and above, with log category b2bgw, and error log level and above withr log category mpgw) to the message group B2B

Similarly, remove a message from a message group by adding the line:

-.messageGropName.syslogMessageCode=logLevel.logCategory,logLevel.logCategory,logLevel.logCategory

For example:
-.MemActionLevel.0x80e0013f=debug.memory-report
Will remove the message 0x80e0013f (debug log level and above, with log category memory-report) from the message group MemActionLevel

> Changing message groups setting may have tremendous impact on DPOD performance, DPOD functionality and also on network utilization. Supporting customers for performance issue will be performing on default message group setting only.

Customize

The Customize section under **[ManageCustomize]** provides access to the management screens for DPOD's Dashboards Editor and System Parameters.

- Dashboards Editor
- System Parameters

DASHBOARDS EDITOR

The screen is accessible by clicking **[ManageCustomizeDashboards Editor]** from the The Navigation Bar.

Custom Dashboards Table

All the custom dashboards that are defined in the system are listed in a table. Each row in the table contains the following information for a single custom dashboard:

Column	Description
Name	The custom dashboard's name.
Description	The description for this custom dashboard
Enabled	Whether this custom dashboard is available to all users from the Dashboards menu.

Adding a Custom Dashboard

Click the **New** button on top of the custom dashboards table to add a new custom dashboard in the system.

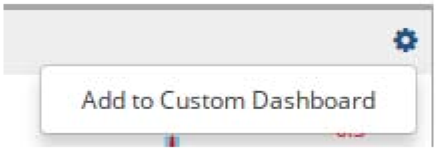
You will need to set the custom dashboard's name, description and whether it's enabled.

Reordering Custom Dashboards

Each row in the table contains the **Move Up** button which allows reordering the custom dashboards, this will effect the order in which the custom dashboards are displayed in the custom dashboard's menu.

Adding Widgets to Custom Dashboard

All charts and grids (widgets) that are part of the dashboards section, have a settings button located at the top right side which includes among other actions, "Add to Custom Dashboard".



Editing Custom Dashboards

Each row in the table contains the **Edit** button which will load the Custom Dashboard Edit screen and provide access to system actions for the custom dashboard.

Custom Dashboard Edit

The Custom Dashboard Edit screen is loaded for a custom dashboard when the **Edit** button is clicked from the Custom Dashboards Table described above.

The system displays the following details:

Detail	Content Description
Name	The custom dashboard's name
Description	A description attached to this custom dashboard
Enabled	Whether this custom dashboard is available to all users from the Dashboards menu.
Widgets in Custom Dashboard	Displays all widgets in this custom dashboard.

You may alter the custom dashboard's name, description and whether it's available to all users.

Edit and Preview Custom Dashboard's widgets

By clicking the **Edit** button, you may use the controls to **resize/move** and **remove** widgets from the custom dashboard.

Resize:

- Resize is done by clicking and dragging the right/bottom side of the widget while the mouse button is pressed.

- The width is calculated in percentage and the height in pixels.
- Each widget has a min-width and min-height, resizing below those values isn't possible.

Move:

- Moving the widget is possible by clicking on the header and dragging the widget while the mouse button is pressed.

Remove:

- Removing the widget is possible by clicking on the trash icon in the header.

Before updating the changes, click the **Preview** button to get a picture of what the custom dashboard will look like.
The UI is responsive which means that the widgets will fill the available horizontal space.

Delete a Custom Dashboard

Click the **Delete** button to remove the custom dashboard from the system.

SYSTEM PARAMETERS

(See Parameters Reference for a complete list of the available system parameters and their usage.)

The System Parameters screen lets you view or change system parameters. The active system parameters are displayed in a table.
Each row in the table contains the following details for a single system parameter:

Column	Description
Name	The system parameter's display name
Category	The system parameter's category
Value	The current value of the system parameter

Changing a System Parameter Value

To edit a system parameter's value, click the parameter's name from the table.

The system will display the parameter in the Edit System Parameter screen.

Edit System Parameter Screen

The screen displays the system parameter's category, name and display name, alongside an input box for the value. If the system parameter has a current value - this value will be displayed in the input box.

1. Change the value to the new value
2. Click the **Update** button
3. A 'Parameter updated successfully' message should be displayed.

Note: The name of the parameter is a system identifier. The display name is much more descriptive and user-readable.

Security Management

The Security section under **[ManageSecurity]** provides access to the management screens for the Users, Groups and Role-Based managed security mechanism provided by DPOD.

Local User Registry (Internal Database Registry)

When DPOD is not configured to use LDAP and the Local User Registry is disabled in system parameters, DPOD will not allow to add or edit any users, roles or groups, the following error message will be displayed:

You can turn the Local User Registry on or off from the system parameters page.

For further information see Security .

USERS

The screen is accessible by clicking **[ManageSecurityUsers]** from The Navigation Bar.

> The users management screen is only available when managing users using DPOD internal database registry. It is not available when DPOD is configured to use LDAP.

Users Table

All the users defined in the system are listed in a table. Each row in the table contains the following information for a single user:

Column	Description
Name	The user name. Clicking on a user's name will load the user's details in the User View and provide access to system actions for the user.
Description	The description for this user

Adding a User

The users table screen contains the **Add User** button at the top.

Click this button to add a new user in the system.

You will need to set the user's name, password and description.

User View

The user view is loaded for a user when the user's name is clicked from the Users Table described above.

The system displays the following details:

Detail	Content Description
User Name	The user's name
Description	A description attached to this user
Groups	This widget lists the Security Groups assigned to this user. You may use the controls in this widget to terminate the user's membership in a group or add them to a new one. Clicking a group's name will open the Group View for the selected group (See Security Groups).
Roles	This widget lists the Security Roles assigned to this user. You may use the controls in this widget to remove a role association or assign the user a new one. Clicking a role's name will open the Role View for the selected role (See Security Roles).

Edit or Delete a User

The User View screen contains two buttons at the top.

Click the **Edit** button to edit the displayed user details. You may alter the user's name, description and password.

Click the **Delete User** button to remove the user from the system.

SECURITY GROUPS

The screen is accessible by clicking **[ManageSecurityGroups]** from the The Navigation Bar.

> The security groups management screen is only available when managing users using DPOD internal database registry. It is not available when DPOD is configured to use LDAP.

Groups Table

All the groups defined in the system are listed in a table. Each row in the table contains the following information for a single group:

Column	Description
Name	The group's name. Clicking on a group's name will load the group's details in the Group View and provide access to system actions for the group.
Description	The description for this group

Adding a Group

The groups table screen contains the **Add Group** button at the top.
Click this button to add a new group in the system.

You will need to set the group's name and description.

Group View

The group view is loaded for a group when the user's name is clicked from the Groups Table described above.

The system displays the following details:

Detail	Content Description
Name	The group's name
Description	A description attached to this group
Users in Group	This widget lists all Users in this group. You may use the controls in this widget to remove users from the group or add new users to it. Clicking a username will open the User View for the selected user (See Users)
Roles of Group	This widget lists the Security Roles assigned to this group (and inherited by members of the group) You may use the controls in this widget to remove a role association or add roles to the group. Clicking a role's name will open the Role View for the selected role (See Security Roles)

Edit or Delete a Group

The Group View screen contains two buttons at the top.

Click the **Edit** button to edit the displayed group's details. You may alter the group's name and description.

Click the **Delete Group** button to remove the group from the system.

SECURITY ROLES

The screen is accessible by clicking **[ManageSecurityRoles]** from The Navigation Bar.

> The security roles management screen is always available, regardless of whether the system is managing users using DPOD internal database registry or LDAP.

Security roles are used to provide a means for the administrator to filter the view users have of the system. Administrators can use the roles to restrict actions and filter out devices, domains, services, client IP addresses, payload and more from a user's view, thereby providing each user with insights to only the parts of the system they are allowed to access.

There are two types of security roles available with DPOD:

- **Built-in Roles** - DPOD's own built-in roles, which can not be added, deleted or altered.
- **Custom Roles** - defined by the administrator. These roles may be added, deleted or altered by a DPOD Administrator.

For a detailed explanation about security roles, see Role Based Access Control.

Custom Roles Table

The custom roles widget at the top of the screen lists the custom roles defined in the system in a table. Each row in the table contains the following information for a single role:

Column	Description
Name	The role's name. Clicking on a role's name will load the role's details in the Role View and provide access to system actions for the role.
Description	The description for this role

Adding a Custom Role

The custom roles table widget contains the **Add Custom Role** button at the top.
Click this button to add a new custom role in the system.

The Role Details section below provides information about the details required for adding or editing custom roles.

Built-In Roles Table

The built-in roles widget at the top of the screen lists the built-in roles defined in the system in a table. Each row in the table contains the following information for a single role:

Column	Description
Name	The role's name. Clicking on a role's name will load the role's details in the Role View and provide access to system actions for the role.
Description	The description for this role

Role View

The role view is loaded for a role when the role's name is clicked from the Built-In Roles Table described above.

The system displays the following details:

Detail	Content Description
Name	The name of this role
Description	The description of this role.
Groups in Role	This widget lists all the Security Groups assigned to this role. You may use the controls in this widget to remove or add a group association to this role. **If you are using an LDAP user registry, please use the LDAP group name.**

Users in Role	This widget lists all the Users assigned to this role. You may use the controls in this widget to remove or add a user association to this role. **If you are using an LDAP user registry, please use the authenticated LDAP user name.**

Custom Role View

The custom role view is loaded for a role when the role's name is clicked from the Custom Roles Table described above.

The system displays the following details:

Detail	Content Description
Name	The name of this role
Description	The description of this role.
Actions and Permissions	
Allow Access to Raw Messages	Whether this role, when assigned to a user, allows them to view Raw Messages.
Allow Access to Payload	Whether this role, when assigned to a user, allows them to view Messages Payload.
Allow Manage Payload Capture	Whether this role, when assigned to a user, allows them to manage payload capture.
Allow Validate Remote WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allow Promote Remote WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allow WSDL URL Change	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Validate Local WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Promote Local WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Stop/Start Service	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allowed Resources	
General	Lists of general resources this role provides access to or All if no resources defined (relevant to IDG and API-C data). The resources in this section are "Device" and "Client IP".
DataPower Gateway	Lists of resources this role provides access to or All if no resources defined (relevant only to IDG data). The resources in this section are "Domain" and "Service".
API Connect	Lists of resources this role provides access to or All if no resources defined (relevant only to API-C data). The resources in this section are "Catalog Name", "Space Name", "Plan Name", "API Name", "Product Name", "Consumer Org Name" and "Client ID".
Denied Resources	
General	Lists of general resources this role denies access to or None if no resources defined (relevant to IDG and API-C data). The resources in this section are "Device" and "Client IP".
DataPower Gateway	Lists of resources this role denies access to or None if no resources defined (relevant only to IDG data). The resources in this section are "Domain" and "Service".
API Connect	Lists of resources this role denies access to or None if no resources defined (relevant only to API-C data). The resources in this section are "Catalog Name", "Space Name", "Plan Name", "API Name", "Product Name", "Consumer Org Name" and "Client ID".

Groups in Role	This widget lists all the Security Groups assigned to this role. You may use the controls in this widget to remove or add a group association to this role. **If you are using an LDAP user registry, please use the LDAP group name.**
Users in Role	This widget lists all the Users assigned to this role. You may use the controls in this widget to remove or add a user association to this role. **If you are using an LDAP user registry, please use the authenticated LDAP user name.**

Edit or Delete a Custom Role

When viewing the details of a customer role, the Role View screen contains two buttons at the top.

Click the **Edit** button to edit the displayed role's details.

Click the **Delete Custom Role** button to remove the custom role from the system.

Role Details

When adding or editing a custom role, you will need to provide the following details:

Detail	Content Description
Name	The name of this role
Description	The description of this role.
Actions and Permissions	
Allow Access to Raw Messages	Whether this role, when assigned to a user, allows them to view Raw Messages.
Allow Access to Payload	Whether this role, when assigned to a user, allows them to view Messages Payload.
Allow Manage Payload Capture	Whether this role, when assigned to a user, allows them to manage payload capture.
Allow Validate Remote WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allow Promote Remote WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allow WSDL URL Change	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Validate Local WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Promote Local WSDL	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Stop/Start Service	Whether this role, when assigned to a user, allows them to perfrom the action in DevOps Services List
Allowed Resources	
General	Lists of general resources this role provides access to or All if no resources defined (relevant to IDG and API-C data). The resources in this section are "Device" and "Client IP".
DataPower Gateway	Lists of resources this role provides access to or All if no resources defined (relevant only to IDG data). The resources in this section are "Domain" and "Service".
API Connect	Lists of resources this role provides access to or All if no resources defined (relevant only to API-C data). The resources in this section are "Catalog Name", "Space Name", "Plan Name", "API Name", "Product Name", "Consumer Org Name" and "Client ID".

Denied Resources	
General	Lists of general resources this role denies access to or None if no resources defined (relevant to IDG and API-C data). The resources in this section are "Device" and "Client IP".
DataPower Gateway	Lists of resources this role denies access to or None if no resources defined (relevant only to IDG data). The resources in this section are "Domain" and "Service".
API Connect	Lists of resources this role denies access to or None if no resources defined (relevant only to API-C data). The resources in this section are "Catalog Name", "Space Name", "Plan Name", "API Name", "Product Name", "Consumer Org Name" and "Client ID".

System Management

The System section under **[ManageSystem]** provides access to the management screens for DPOD's software license.

- License

LICENSE

The License Screen, allows you to view current license details, request a renewal or replacement license, or update the installation with a provided activation license.

The details displayed in the screen are:

Field	Description
License Owner	The license owner's name. This will normally be the name of your organization
Email Address	Licenses are sent by email. When you request a new or replacement license, this is the email address the license will be sent to.
License Type	Different Deployment Scenarios may require a different license. Select to 'All-In-One' unless advised otherwise by DPOD's support.
Expiry Date	The date this license will expire. This depends on your purchase agreement.
Amount of Devices	Maximum number of monitored devices you can configure. This depends on your purchase agreement.

Request or Update License

The License Screen contains two buttons at the top.

Click the **Request License** button to generate a new license request. You will need to provide the details above and generate a request key, which you'll need to
email DPOD's support in order to receive a new license (See Activate License for further details).

Click the **Update License** button to update the system when a new license key has been emailed to you.

A complete description of the license activation process is available at Activate License.

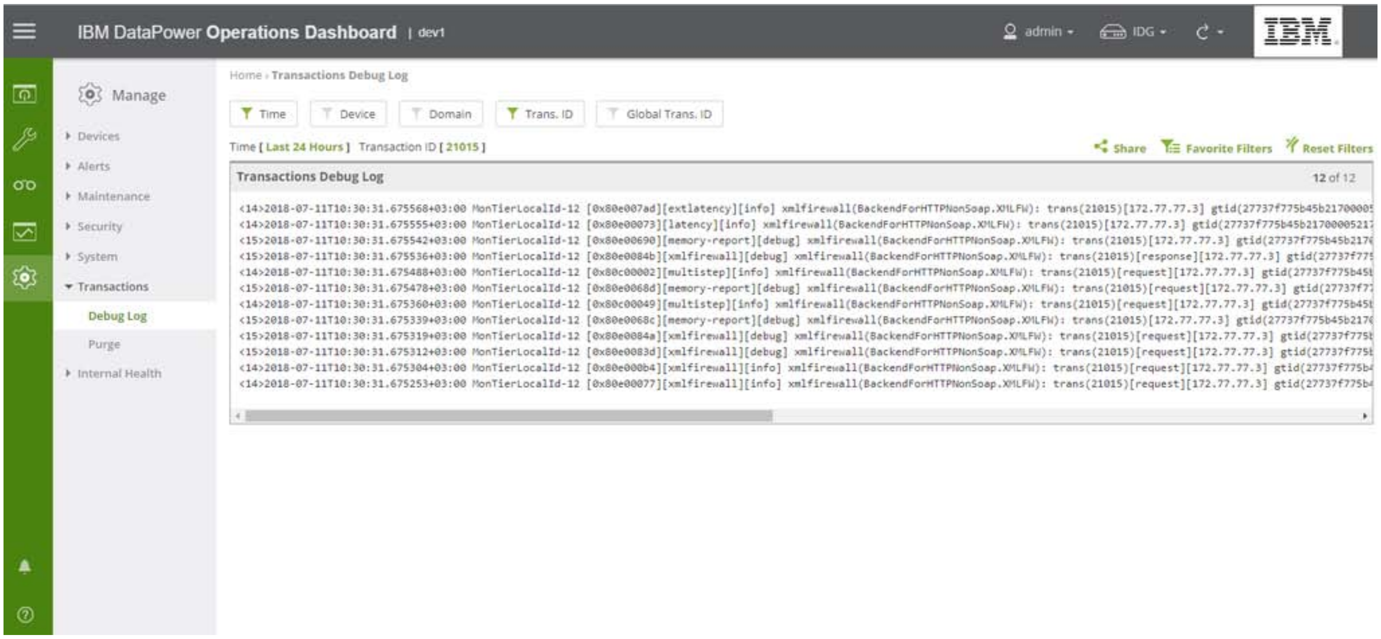
Transactions

The Transactions section under [ManageTransactions] provides access to a set of tools which let the user view,analyze and delete transaction logs from Store.

- Transaction Debug Log
- Transaction Purge

TRANSACTION DEBUG LOG

This page may be used to view all raw syslog messages (up to 1500 syslogs) for a certain transaction ID, Global Transaction ID, or all latest syslogs for a device or a domain.



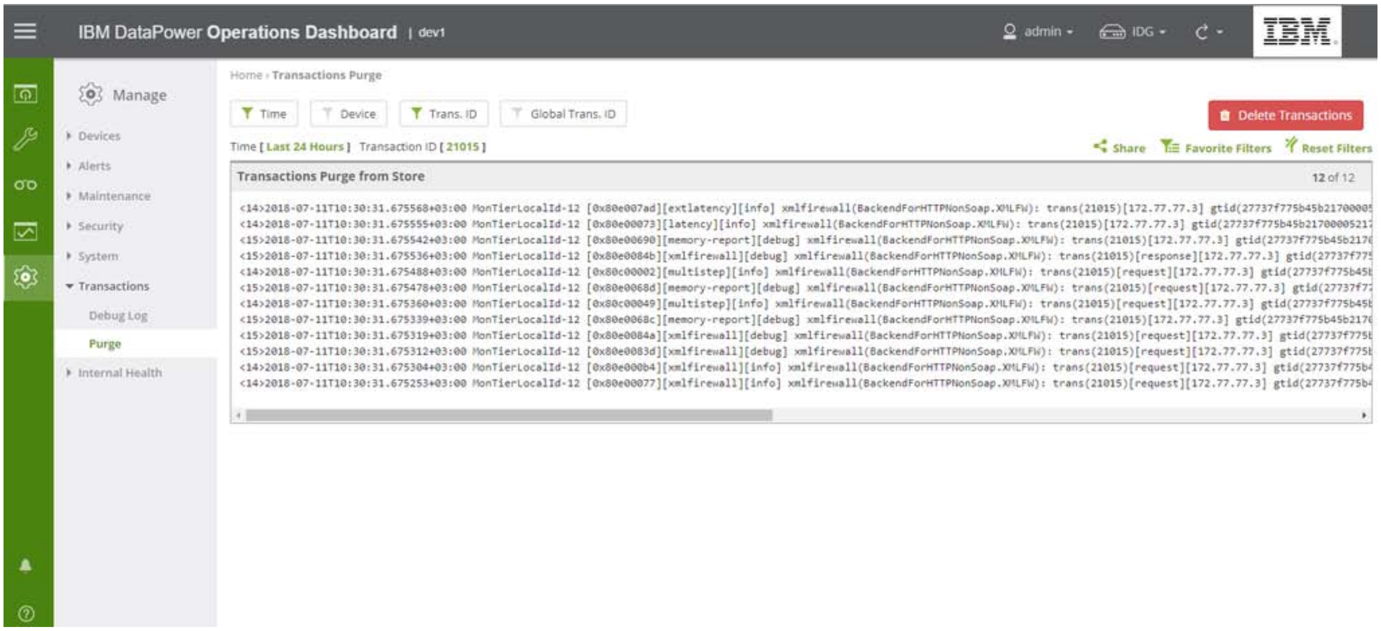
Time [Last 24 Hours] Transaction ID [21015]

Transactions Debug Log 12 of 12

```
<14>2018-07-11T10:30:31.675568+03:00 MonTierLocalId-12 [0x80e007ad][extlatency][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b2170000
<14>2018-07-11T10:30:31.675555+03:00 MonTierLocalId-12 [0x80e00073][latency][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b217000052
<15>2018-07-11T10:30:31.675542+03:00 MonTierLocalId-12 [0x80e00690][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b217
<15>2018-07-11T10:30:31.675536+03:00 MonTierLocalId-12 [0x80e0084b][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[response][172.77.77.3] gtid(27737f77
<14>2018-07-11T10:30:31.675488+03:00 MonTierLocalId-12 [0x80c00002][multistep][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b45
<15>2018-07-11T10:30:31.675478+03:00 MonTierLocalId-12 [0x80e0068d][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f7
<14>2018-07-11T10:30:31.675360+03:00 MonTierLocalId-12 [0x80c00049][multistep][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b45
<15>2018-07-11T10:30:31.675339+03:00 MonTierLocalId-12 [0x80e0068c][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b217
<15>2018-07-11T10:30:31.675319+03:00 MonTierLocalId-12 [0x80e0084a][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775
<15>2018-07-11T10:30:31.675312+03:00 MonTierLocalId-12 [0x80e0083d][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775
<14>2018-07-11T10:30:31.675304+03:00 MonTierLocalId-12 [0x80e000b4][xmlfirewall][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b
<14>2018-07-11T10:30:31.675253+03:00 MonTierLocalId-12 [0x80e00077][xmlfirewall][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b
```

TRANSACTION PURGE

This page may be used to purge transactions from Store, it is mandatory to choose a transaction ID or a global transaction ID.



Time [Last 24 Hours] Transaction ID [21015]

Transactions Purge from Store

12 of 12

```
<14>2018-07-11T10:30:31.675568+03:00 MonTierLocalId-12 [0x80e007ad][extlatency][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b2170000
<14>2018-07-11T10:30:31.675555+03:00 MonTierLocalId-12 [0x80e00073][latency][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b2170000521
<15>2018-07-11T10:30:31.675542+03:00 MonTierLocalId-12 [0x80e00690][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b217
<15>2018-07-11T10:30:31.675536+03:00 MonTierLocalId-12 [0x80e0084b][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[response][172.77.77.3] gtid(27737f775
<14>2018-07-11T10:30:31.675488+03:00 MonTierLocalId-12 [0x80c00002][multistep][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b45
<15>2018-07-11T10:30:31.675478+03:00 MonTierLocalId-12 [0x80e0068d][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f77
<14>2018-07-11T10:30:31.675360+03:00 MonTierLocalId-12 [0x80c00049][multistep][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b45
<15>2018-07-11T10:30:31.675339+03:00 MonTierLocalId-12 [0x80e0068c][memory-report][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[172.77.77.3] gtid(27737f775b45b217
<15>2018-07-11T10:30:31.675319+03:00 MonTierLocalId-12 [0x80e0084a][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775
<15>2018-07-11T10:30:31.675312+03:00 MonTierLocalId-12 [0x80e0083d][xmlfirewall][debug] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775
<14>2018-07-11T10:30:31.675304+03:00 MonTierLocalId-12 [0x80e000b4][xmlfirewall][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b
<14>2018-07-11T10:30:31.675253+03:00 MonTierLocalId-12 [0x80e00077][xmlfirewall][info] xmlfirewall(BackendForHTTPNonSoap.XMLFW): trans(21015)[request][172.77.77.3] gtid(27737f775b
```

Internal Health

The Internal Health section under [ManageInternal Health] provides access to a set of tools which let the user view and analyze the overall system status and health.

- Internal Health Alerts
- Agents
- Devices
- Store
- Operating System (OS)

INTERNAL HEALTH ALERTS

DPOD automatically runs several self diagnostic tests (checks) on the following internal components:

- Derby Database availability
- ElasticSearch (the Big Data Store) availability
- File system free space
- Internal Big Data Retention process
- Dropped syslog messages
- Dropped WS-M messages
- Syslog and WS-M agent status

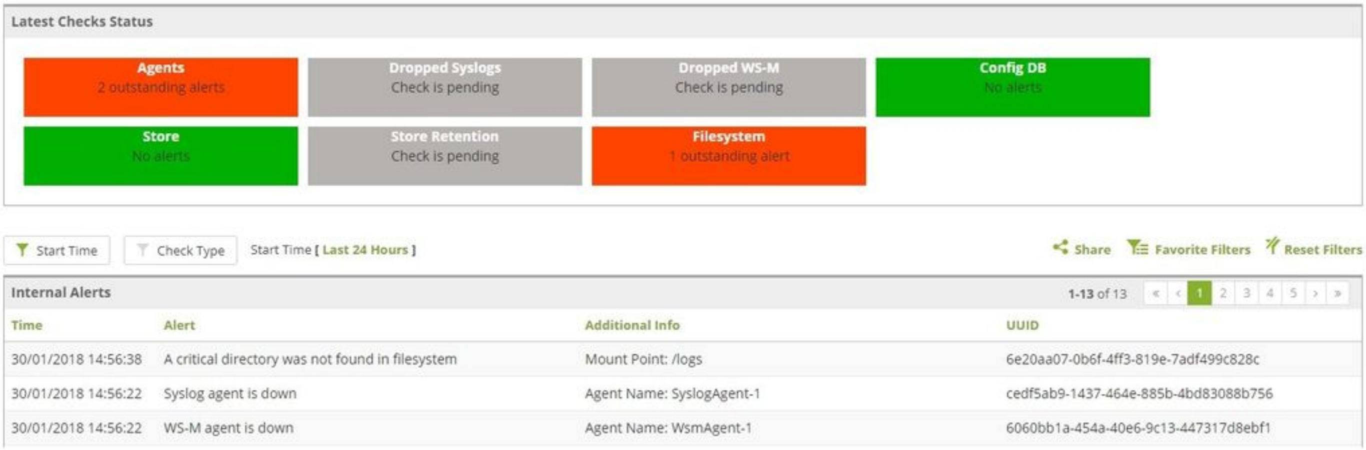
> You can turn off some or all of the checks from by logging in to your DPOD server (via ssh), editing the file:
> /app/hk_keepalive/MonTier-HK-SyslogKeepalive/conf/MonTierHousekeeping.conf
> and restarting the keepalive service via app-util.sh

The internal alerts can be published in three ways:

1. Via Email - from the system parameters page, change the value of "Internal Alerts - Send Email on Alert" to "true", and enter the email destination/s (comma separated) in "Internal Alerts - Email Destination Address for Alerts" - you'll need to restart the keepalive service via app-util.sh for the change to take effect
2. Via Syslog - from the system parameters page, change the value of "Internal Alerts - Send Syslog on Alert" to "true", the syslog destination is identical to the destination of the normal system alerts, and can be configured from the parameters "Hostname of the target server for syslog alerts" and "Port of the target server for syslog alerts" - you'll need to restart the keepalive service via app-util.sh for the changes to take effect
3. As a notification in the web console, you can change the interval of the alerts from the user preferences page

Internal Alerts Page

The internal alerts page showing current and historic alerts.



Latest Checks Status

Agents 2 outstanding alerts	Dropped Syslogs Check is pending	Dropped WS-M Check is pending	Config DB No alerts
Store No alerts	Store Retention Check is pending	Filesystem 1 outstanding alert	

Internal Alerts

1-13 of 13

Time	Alert	Additional Info	UUID
30/01/2018 14:56:38	A critical directory was not found in filesystem	Mount Point: /logs	6e20aa07-0b6f-4ff3-819e-7adf499c828c
30/01/2018 14:56:22	Syslog agent is down	Agent Name: SyslogAgent-1	cedf5ab9-1437-464e-885b-4bd83088b756
30/01/2018 14:56:22	WS-M agent is down	Agent Name: WsmAgent-1	6060bb1a-454a-40e6-9c13-447317d8ebf1

The page is divided into two sections - the top section shows the status of each check
Green - No problems detected
Red - One or more issues were detected, or the previous schedule check did not run (because of a problem with DPOD for example), but a previous check detected a problem.
Grey - The check did not run yet - some checks only start a few minutes to an hour after DPOD starts up - this is normal and does not indicate on any problems.

The bottom section shows a table with all the alerts (current and historical)

Name	Description
Time	The time where the internal alert was generated
Alert	Description of the internal alert - for example "Syslog agent is down"
Additional info	Any other diagnostic information - for example "Agent Name: SyslogAgent-1"
UUID	An internal UUID , you can search for this UUID in the logs when instructed to do so by support personal

Internal Alerts Syslogs

See Internal Health Alerts to learn how to turn syslog notifications for internal alerts on and off

Internal Alerts Syslogs Format

```
<16>Mar 14 13:26:22 hostname [0x00a0002a][DPOD-internal-alert][info] AlertContent:(A critical directory was not found in filesystem) AlertUUID:(d44b291e-efda-4236-bd2c-8de0ab1d4e3d) AdditionalInfo:(Mount Point: /logs)
```

The hostname is DPOD server hostname

The message ID for all alerts will always be 0x00a0002a

The message level (info, warn, error, etc) may be set via the system parameters (under "Syslog Severity Field Value")

List of Possible AlertContent Values

Cannot connect to DB
Query failed from DB
Not enough space in mount point
A critical directory was not found in filesystem
Store cluster status is red
Could not connect to the Store
Syslog agent is down
WS-M agent is down
Agent dropped Syslog messages
Agent dropped WS-M messages
The Store retention process is not working
Database table exceeding threshold size

AGENTS

The Agents screen is accessible by logging into the Web Console and navigating to **[ManageInternal HealthAgents]**.

DPOD agents are responsible for collecting data (either actively or passively) from monitored devices and storing it in the Big Data Store. This screen allows you to verify that the agents are up and running.

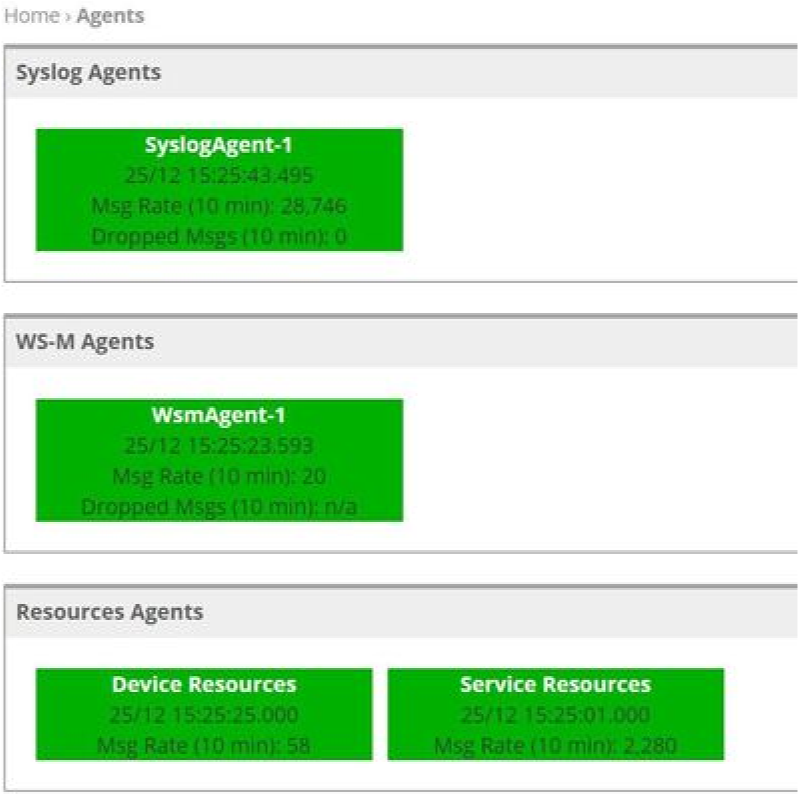
The screen shows two sections:

1. **Agent Status** - Showing the state of all the agents
2. **Agent Processing Status-** Showing streaming and memory consumption data

Agent Status

The Agent Status section of the screen is a set of 3 widgets, each displaying data related to a different set of DPOD Agents: **Syslog, WS-M** and **Resources.** The agents are monitored internally by a KeepAlive service. For a list of all system services, and an explanation on KeepAlive processing, see section on System Services Management.

Each collector agent is displayed in a colored box (see below). Click an agent's name to open its details in the Agent's Detail view.



SyslogAgent-1
25/12 15:25:43.495
Msg Rate (10 min): 28,746
Dropped Msgs (10 min): 0

WsmAgent-1
25/12 15:25:23.593
Msg Rate (10 min): 20
Dropped Msgs (10 min): n/a

Device Resources
25/12 15:25:25.000
Msg Rate (10 min): 58

Service Resources
25/12 15:25:01.000
Msg Rate (10 min): 2,280

The table below describes the details presented for each agent:

Detail	Description	Desired State

General Health Status	The general health status of the agent is relayed by the color of the box wrapping its details. • **Green** – The agent is running and is ready to receive and store syslog messages (Keepalive checks were successful) • **Yellow** – Syslog records or Keepalive checks did not arrived in the last 3 minutes OR number of dropped records is greater than 0. • **Red –** Syslog records or Keepalive checks did not arrived in the last 10 minutes or more. • **Grey** - Device/Service Resources agents only. No monitored devices were added yet, or device/service resource monitoring wasn't requested for any device (this status does not indicate any problem) Possible agent issues : • Monitored device system time that is **not** synced with DPOD's system time could send Syslog record with "future" time that will cause the agent's health status to be **Yellow** or **Red.** • The agent service is down - Syslog records and Keepalive records will be processed causing the agent's status to change to **Yellow** or **Red**. • The Keepalive service is down - Syslog agent did not receive any records from monitored device, this will cause the agent's status to change to **Yellow** or **Red**.	Green - the agent is healthy.
Date / Time	The timestamp of the last successful record processed by the agent (Syslog record or Keepalive check). A delay of over a minute may suggest a performance problem. Note: It is important to verify that system time is time synced correctly when reading these values.	< 3 minutes
Msg. Rate	This is the total number of messages of all types (syslog, WS-M, and keepalive messages) processed by this agent in the last 10 minutes. Verify: • That the number is greater than 1. If it isn't, either agents are down or the network is down. • For Syslog agents: the number should reflect the expected throughput of raw logs records received from all monitored devices in the last 10 minutes. • For WS-M agents: If WS-M recording is enabled, the number should reflect the message throughput for the recording service/domain in 10 minutes. • If this value is more than 500,000 consider redistributing traffic to other agents, in order to optimize performance You may redirect syslog traffic from one agent to another by assigning it to a domain a specific agent. For more details see Adding Monitored Devices.	1 < value < 500,000 (if there are any monitored devices)
Dropped Msgs (For Syslog and WS-M agents)	This is the total number of syslog or WS-M messages that were sent from the monitored devices but were not processed by the DPOD agent in the last 10 minutes. Dropped messages usually indicate that the agent cannot keep up with the load, consider redistribution of traffic to other agents.	0

If you encounter any problems, see how to Troubleshoot links to agent status troubleshooting.

Agents processing status

The bottom of the screen displays the agents processing status graphs, which relay the state of processing agents.

Graph	Details	Desired State
Files Process Pending	The graph depicts the number of large payloads waiting to be processed. A value higher than 1000 indicates a high load on WS-M subscription. WS-M usage should be avoided until this folder is cleared by the system or you clear it manually.	Only a few files displayed
Channel Utilization	The graph depicts stream processing usage in percentage. Each colored graph denotes a different agent. Verify that all agents use less than 80% of their stream processing capacity. If usage goes above 80%, data coming in from collector agents might be lost. See how to Troubleshoot the issue.	Under 80% for all agents
Agents Free Memory	The graph depicts the collector agents' free memory over time, where each agent is denoted in a different color. When an agent's free memory is too low, you might encounter performance problems. See how to Troubleshoot the issue.	Verify that each agent has at least 30-40 Mil free.

Agent's Detail View

When clicking an agent name on the Agent Status screen, DPOD opens the agent's details in a single-agent details view.

The Agent Details view is composed of 4 widgets (for syslog and WS-M Agents) or 3 widgets (for Resources Agents).

Agent Details

The agent details widget displays the following information for the agent:

Detail	Description
IP	The IP where this agent runs
DNS	The DNS of the agent (if set)
Port	The port the agent is listening on
Keepalive	On / Off state of the keepalive service for this agent
Dropped Msgs (10 mins)	How many messages were lost by the agent
Message Rate (10 min)	Number of messages handles by agent in the last 10 minutes
Newest Message	Timestamp of the latest message received on this agent

Recent Keep-Alive Messages

This widget displays a table with details of recent keep-alive messages received on this agent. Scanning this table for changes in frequency may help catching issues.

The following information is displayed for each message:

Column	Description
Device	The device emitting the message. Click on the device name to view the device in the Raw Messages view.
Domain	The domain for this message
Category	Always montier-ka
Severity	Always debug
Time	Timestamp for the Keep-Alive message
Direction	N/A
Object Type	N/A
Object Name	N/A
Trans. ID	N/A
Client IP	This will always be the originating host so 0.0.0.0
Message	Keep-Alive message text.

Agent Statistics

Graph	Description
Message Rate (per sec)	This widget displays a graph of the number of messages per second going through this agent over the last 24 hours period
Dropped Syslog Messages	This graph shows the number of messages dropped by the agent. This value is cumulative , the agent will reset it to zero only after restart.

Channels Utilization	The graph depicts stream processing usage of the current agent in percentage.
Free Memory	The graph depicts the collector agent free memory over time.

Reporting Domains (24 hrs.)

This widget lists the domains reporting in the preceding 24 hours period.
The list may be used to identify that a device has dropped off the monitoring list.

Column	Description
Device Name	Name of reporting device
Domain Name	Name of reporting domain

Recent Resources Messages

This widget displays only for the Device and Service Resources Agents. It lists recent resource messages in a table.
Resource messages are status messages where the resource relays the status of its resource consumption.

For each resource message, the table displays the following details:

Column	Description
Device ID	ID of the device this resource message relates to
Device Name	Name of the device this resource message relates to
Load Time	Timestamp when the load sampling was taken
Load	Load sampling value
Memory Time	Timestamp when the memory sampling was taken
Used Memory	Memory used sampling value
Total Memory	Total memory for the device
Total Memory %	Percentage of total memory used at sampling time
CPU Time	Timestamp when the CPU usage sampling was taken
CPU	CPU usage (%) at sampling time

Monitored Devices (24 hrs.)

This widget displays only for the Device and Service Resources Agents. It lists the devices monitored by DPOD in the preceding 24 hours period.
The list may be used to identify that a device has dropped off the monitoring list.

DEVICES

The Devices screen is accessible by logging into the Web Console and navigating to **[ManageInternal HealthDevices]**

The screen contains two tables displaying details about your Data Power devices log targets and WSM Agents.

Controlling the sampling interval for this screen

You can change the sampling interval for both Logtargets and WSM agents from the System Parameters screen (under the "Health" category)

You may also turn the sampling on or off by setting the parameter value to "true" or "false".

The default for both is to sample every 300 seconds.

Log Targets Stats

The Log Targets Stats table shows details about DPOD's logtargets on all your monitored devices.

Details	Description
Device / Domain / LogTarget	The names of the monitored device, domain and logtarget. DPOD creates two logtargets for each domain (except for the default domain which has one logtarget)
Status	The status of the logtarget - e.g. Active, Failure. If the status is not "Active" - you can view more information about the issue from your DataPower's Control Panel, under the "Logging Targets" screen
Events Processed	Number of events processed by this logtarget This value is cumulative, the DataPower will reset it to zero only after the DataPower/Domain was restarted.
Events Dropped	Number of events that were not processed by this logtarget This value is cumulative, the DataPower will reset it to zero only after the DataPower/Domain was restarted.
Events Dropped ~10m	The value of "Events Dropped" from around 10 minutes ago. You can use the delta of this value and "Events Dropped" to determine if the logtarget is currently losing syslog records.
Events Dropped ~1h	The value of "Events Dropped" from around 60 minutes ago. You can use the delta of this value and "Events Dropped" to determine if the logtarget was losing syslog records in the last hour.
Events Dropped ~24h	The value of "Events Dropped" from around 24 hours ago.

WSM Agents Stats

The WSM Agents Stats table shows details about the WSM Agents on all of your monitored DataPower devices.

Details	Description
Device / Domain	The names of the monitored device and domain
Spooler Count	How many WSM subscribers are active for this domain

Records Seen	Total number of records processed by this agent This value is cumulative, the DataPower will reset it to zero only after the DataPower/Domain was restarted.
Pending Records	Records waiting to be processed by this agent
Records Lost	Number of records that were not processed by this agent This value is cumulative, the DataPower will reset it to zero only after the DataPower/Domain was restarted.
Records Lost ~10m	The value of "Records Lost" from around 10 minutes ago. You can use the delta of this value and "Records Lost" to determine if the WSM agent is currently losing records.
Records Lost ~1h	The value of "Records Lost" from around 60 minutes ago. You can use the delta of this value and "Records Lost" to determine if the WSM agent was losing records in the last hour.
Records Lost ~24h	The value of "Records Lost" from around 24 hours ago.

STORE

The Store screen is accessible by logging into the Web Console and navigating to **[ManageInternal HealthStore]**.

DPOD's Big Data Store is where all of DPOD's data is stored.

This screen display consist of 5 widgets, each allowing access to view data or perform Store-related tasks. They are described below and in the following pages:

- Pending Tasks
- Delete Stored Data Operations

Health Data

The top 3 widgets display health data related to the store.

Cluster Status

Detail	Description	Desired State
ex-raw-trans	The general state of the Big Data store. • **GREEN** – Everything is working properly. • **YELLOW** – System is up and running, but there's a problem requiring your attention (e.g. one of the nodes is down, but another node took over) • **RED** – There is a major problem with the Big Data store. DPOD functions are offline. Contact support. Note: During the first 10-20 minutes following a system startup, a value of **YELLOW** or **RED** is normal.	**GREEN** (but **RED** and **YELLOW** acceptable during startup)
Shards	Details of the allocation of logical data to physical storage in the Big Data Store. All shards should be **assigned**, and unassigned shards number should be 0. Note: During the first 10-20 minutes following a system startup, a value greater than zero is normal. If unassigned shards persist, see Unassigned Shards under troubleshooting.	0 Unassigned shards. (but a larger than 0 value acceptable during startup)
Buttons	Two buttons are available to the far right of the cluster status widget. Both the ES-head and ES-Visualize buttons are for DPOD support troubleshooting tasks. When required, DPOD support will guide you through the usage of these buttons.	

Index Sets

Data sets that store monitoring data received from monitored devices.

Detail	Description	Desired State
Name	Index name	n/a
Indices Count	Indices counts should be about 1 per day or at most 2 per day. The number of days stored in an index set can be derived by finding the delta in days between the oldest and newest document time stored inside it. The indices count should therefore be no more than twice that value. When the Indices count is higher, query performance may be affected. See Increase Storage for Index Sets for ways to resolve this.	At most - twice the number of days stored in data set.
Size	Size of the data set.	Each index should contains data between 1 day to 2 maximum
Documents Count	All data sets starting with "**wdp-**" should have a document count larger than 0. A value of 0 for a **wdp-*** data set points to problems receiving data from monitored devices.	> 0
Oldest Document Time	Oldest record in the index set. Verify that this fits your requirements, and if not – you may need to Increase Storage for Index Sets.	As per your requirements

Newest Document Time	Newest record in the index set. Verify that this fits your requirements, and if not – you may need to Increase Storage for Index Sets.	As per your requirements

DPOD uses index sets to manage different data types in the Big Data store.

Index set Name	Description
wdp-syslog	Contains log records collected by the Syslog agents from monitored devices, except system messages – e.g. transaction started, network call states, integration code errors, etc.
wdp-syslog-sys-*	Contains log records of system events collected by the Syslog agent from monitored devices.
wdp-wsm	Contains payload message collected by the WS-M agent when WS-M recording is enabled.
wdp-device-resources	Contains data collected by the device resources agent, e.g. monitored devices CPU, memory, hardware state, etc.
wdp-service-resources	Contains data collected by the service resources agent, e.g. memory consumption by monitored services, etc.

Other index sets are restricted and are for internal use only.

These indexes are self-managed from a disk storage perspective. Each index set is divided into multiple indexes and when the allocated space for that index set is exhausted, the oldest index set is deleted and new one is created.
This operation is done by the retention housekeeping process.

Nodes

These are the data nodes which the store uses for its internal processing.

Detail	Description	Desired State
Name	Node Name	n/a
Version	Node Version	n/a
Host Name	Node's host name	n/a
Type	A correctly set up system should have at least one ‘D’ node (data processing node), and an odd number of ‘M’ nodes (master nodes).	• D Nodes > 0 • Odd M Nodes number

Nodes Health

The Nodes Health table contains additional information about the ElasticSearch nodes (for example, the amount of swap space used, average time to index documents, etc)
Hover over the data to get additional information.

Pending Tasks

This Table show a list of Pending task while Store initialize or perform other administrative tasks.

Tasks appears in list for a while can indicate a problem in the Store

https://www.elastic.co/guide/en/elasticsearch/reference/current/cluster-pending.html

Delete Stored Data Operations

This widget appears on the Store management screen, and lets the user perform operations to purge various sections of DPOD's Big Data Store according to data type, as specified below.

> These are sensitive operations, which might affect your system in unexpected ways. **These operations cannot be rolled back. Do not perform these operations if you are unsure how they will affect your system.**

The only operational situation where deleting an index set is recommended, is when sensitive data was collected using WS-M agents.

To safely delete this sensitive data, first shut down all WS-M Collectors (using the app-util scripts) and then delete the Index set.
Wait for 1-2 minutes until the index set is recreated before you start the WS-M collectors again.

Operation	Description	Usage
Delete Payload (WS-M) Data	Purge payload information recorded by WS-M	User
Delete Syslog TRAN Data	Purge transaction records received via Syslog	User
Delete Syslog SYS ERROR Data	Purge system error records received via Syslog	User
Delete Syslog AUTH Data	Purge system authorization records received via Syslog	User
Delete Syslog DEFAULT Data	Purge system default records received via Syslog(unclassified)	User
Delete DEVICE Resources Data	Purge device resource information recorded by the Device Resource agent	User
Delete SERVICE Resources Data	Purge device resource information recorded by the Service Resource agent	User
Delete Services Configuration Data (ES)	Purge service configuration information recorded by the Service Resource agent	User
Delete Restarts Data	Internal use	SYSTEM Only
Delete Sync Import Results Data	Internal use	SYSTEM Only
Delete Objects Status Data	Internal use	SYSTEM Only
Delete Logical Tran FULL Data	Internal use	SYSTEM Only
Delete Logical Tran COMPACT Data	Internal use	SYSTEM Only
Delete APIC Data	Internal use	SYSTEM Only
Delete IIB Tran Data	Internal use	SYSTEM Only
Delete IIB Stats Data	Internal use	SYSTEM Only
Delete Services Configuration Data (DB)	Internal use	SYSTEM Only
Delete System Health Data	Internal use	SYSTEM Only
Delete Internal Operations Data	Internal use	SYSTEM Only
Delete Static Data	Internal use	SYSTEM Only

For more information on storage locations and capacity, see the index sets descriptions on Store.

OPERATING SYSTEM (OS)

The Operating System screen is accessible by logging into the Web Console and navigating to **[ManageInternal HealthOperating System]**.

The screen contains a table displaying file system information. Verify that the following directories have the required minimum free space:

Root Directory	Min. Free Space Required	Default allocation
/	400 mb	2 GB
/var	2GB	4 GB
/tmp	400mb	1 GB
/app	2 GB	6 GB
/data	10 GB	
/installs (used for updates)	2GB	6GB
/logs	500mb	10GB

All of DPOD's indexes are located in the /data file system. See the index sets description and operations on the Store and Increase Storage for Index Sets pages.

Using the Command Line Interface (CLI)

The Command Line Interface (CLI) allows DPOD administrators to view the status of system services and their vitality alongside system logs and performance metrics.

To start the CLI consult the Run the Main Admin Menu CLI page.

CLI MAIN ADMIN MENU OPERATIONS

The following operations are available via the CLI menu:

Operation	Purpose
Start All System Services	Start all DPOD system services
Stop All	Stop all DPOD system services
Check Status	View DPOD system services status (running/stopped)
Start Service	Start DPOD system services. The command lets you start either single service or a list of several services.
Stop Service	Stop DPOD system services. The command lets you stop either a single service or a list of several services.
MustGather	Create and export DPOD MustGather logs. (This operation may be requested of you by product support) In order to run the command see following link
Reboot Device	Restart the DPOD device (physical or VM)
Shutdown Device	Shutdown the DPOD device (physical or VM)
Upgrade/Update	Upgrade the DPOD installation to a newer version. This requires an update file (Fix file) to be uploaded to the system
Exit	Exit the CLI

System Services Management

DPOD system services are operating system processes performing various processing and maintenance tasks.
Depending on your system's processing profile requirements, some services may have more than a single instance.

DPOD's Internal services are divided into the following groups:

1. **Collector Agents** – These services collect data (either passively or actively by periodic polling) from monitored DataPower Gateways. The data is then and forwarded to DPOD's Big Data Store storage.
2. **Database** – These services host database services for all the data stored in DPOD, (e.g. raw logs and configuration data). Refer to Components for more detail about the database.
3. **Other** – Services which perform various other tasks.

The following tables list the various DPOD's services and their function

COLLECTOR AGENTS

Service Name	Function
Syslog Agent *	Syslog Agents passively receive raw log records from monitored DataPower Gateways, process them and store them into the Big Data Store. The number of process instances for this agent depends on the installation requirements.
Syslog Keepalive	The Syslog Keepalive agent monitors the health of a Syslog Agent. The keepalive agent periodically sends syslog records to the syslog agent, which writes those records to the Big Data Store. The Keepalive agent later verifies the Syslog's agent correct processing by reading those entries from the store and verifying they have been written correctly. **Note: A successful Keepalive check only means that the syslog agent is functioning properly, and that it can be write data to the Big Data store.** **It does not imply that data is being received from monitored devices (keepalive is a local service and will be successful even when the network is down)**
WS-M Agent *	WS-M Agents passively receive message payload information from monitored DataPower Gateways on which WS-M recording has been enabled. Payloads are processed and stored in a dedicated index set inside the Big Data store. The number of process instances for this agent depends on the installation requirements.
WS-M Keepalive	The WS-M Keepalive monitors the health of a WS-M Agent, in the same way that the Syslog Keepalive service above works.
Device Resources Agent	This service periodically polls device resource information from monitored DataPower Gateways. The data polled is resource consumption related and includes metrics for CPU, memory, file system, hardware etc.
Service Resources Agent	This service periodically polls service resource information (e.g memory consumption) and configuration details from monitored DataPower Gateways.

DATABASE

Service Name	Function
Configuration Database	Manages DPOD's internal SQL database used to retain configuration data, agent states etc.
Big-Data data nodes *	Manages various functions of the Big Data Store.
Big-Data data retention	Performs regular maintenance tasks (e.g. for indexes or storage) on the Big Data Store.

Other

Service Name	Function
Console UI	Hosts and manages the web-based Console used to interact with DPOD UI
Reports	Runs and formats user Reports.

*** These agents can have more than one instance, appearing as multiple processes in the operating system.**

Common Administration Tasks

This section deals with common administration tasks in DPOD.

- Run CLI Main Admin Menu
- Check System Services Status with the CLI
- Stop All System Services
- Start All System Services
- Log-in to DPOD Web Console
- Check System Status Using the Web Console
- Change Appliance Network Address
- Increase DPOD's Store Space
- Changing Agents TCP port
- Adding Second Network Interface to DPOD
- Change sampling interval intervals

Run CLI Main Admin Menu

To access the CLI admin menu:

1. Connect to the DPOD Appliance with ssh (or from a console in case of a virtual appliance)
2. Log in and run the following command to start the CLI Main Admin Menu utility

```
app-util.sh
```

If the script execution displays “ERROR: Cannot find properties file”- re-login to the server or use **su -**

When successful, the system will display a menu with all the common admin tasks.
For further information on each option consult Manage Using CLI.

Check System Services Status with the CLI

1. Ensure you are logged in to the Main Admin Menu.
2. Select **Check Status**. The system will echo a list of services and their status.
3. Verify that agents and services are in the correct state, as specified in the table below.

Service/Agent Name	Process Name Example	Desired State
Syslog Agent *	montier-SyslogAgent-1	running
Syslog Keepalive	montier-HK- SyslogKeepalive	running
WS-M Agent *	montier-WsmAgent-1	running
WS-M Keepalive	montier-HK- WsmKeepalive	running
Device Resources	montier-HK-WdpDeviceResources	running
Service Resources	montier-HK-WdpServiceResources	running
Configuration Database	montier-Derby	running
Big-Data data nodes *	montier-es-raw-trans-Node-1	running
Big-Data data retention	montier-HK-ESRetention	running
Console UI	montier-UI	running
Reports	montier-Reports	running

* These agents can have more than one instance, appearing as multiple processes in the operating system.

> A running process does not necessarily mean the service is operational. When in doubt, always consult the keep alive information found in the Agents section of the Web Console.

See Troubleshooting if you encounter any problems

Stop All System Services

1. Ensure you are logged in to the Main Admin Menu.
2. Select **Stop All**.
3. Wait for the system to stop all services.

Start All System Services

1. Ensure you are logged in to the Main Admin Menu.
2. Select **Start All**.
3. Wait for the system to stop all services.

Log-in to DPOD Web Console

Before you begin

You will need:

- A supported browser
- DPOD's IP address
- Network access to DPOD
- Valid username and password

To Login

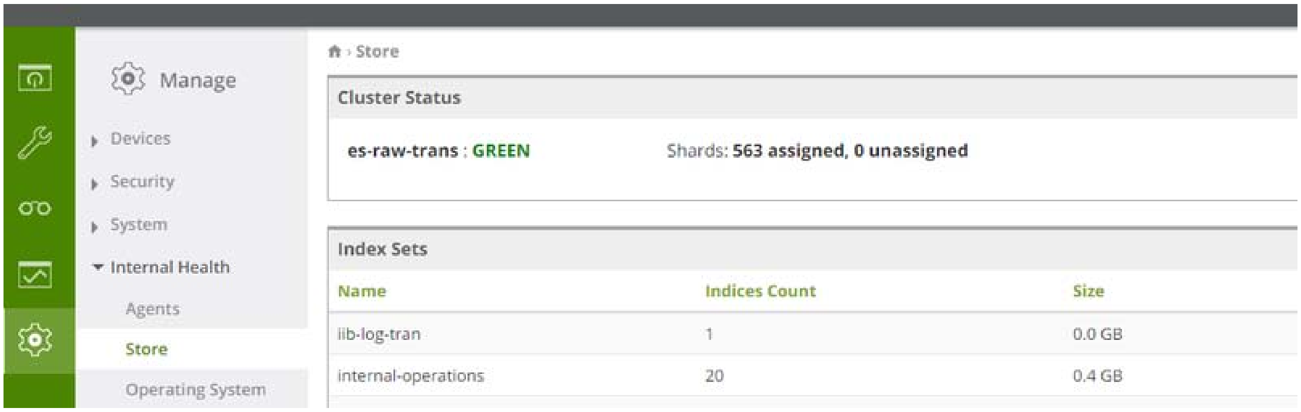
1. Open your browser
2. Enter following URL into the address bar: https:/**<DPOD appliance IP address>**/
3. During installation, DPOD's Web Console is shipped with a self-signed certificate. If the certificate has not been replaced, you might get a security exception in your browser.

   > We encourage you to install your own certificate.

4. Log in with the username and password you have been provided.

Check System Status Using the Web Console

1. Login to the Web Console
2. Select **[Manage->Internal HealthStore]** to open the Store page.



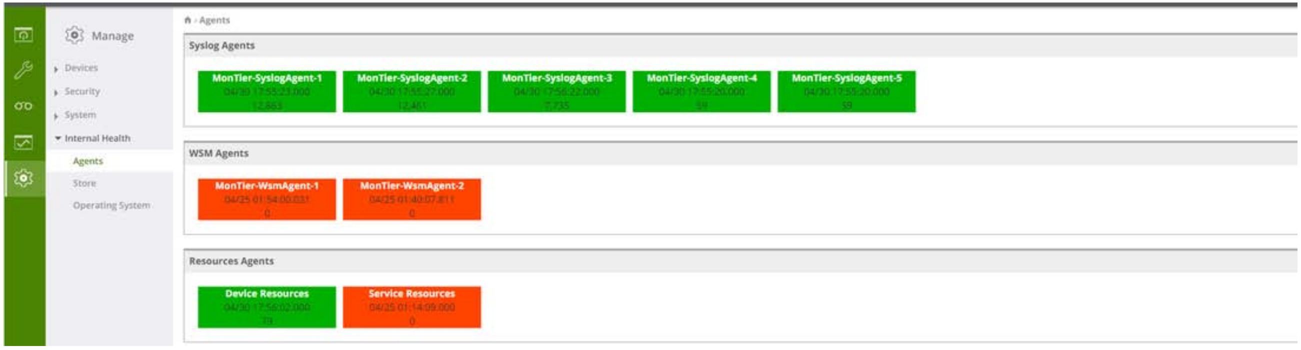
Cluster Status

es-raw-trans : GREEN   Shards: 563 assigned, 0 unassigned

Index Sets

Name	Indices Count	Size
lib-log-tran	1	0.0 GB
internal-operations	20	0.4 GB

3. Verify that the Cluster Status is GREEN and that there are 0 unassigned shards.
4. Select **[Manage->Internal HealthAgents]** to open the Agents page.



Syslog Agents

MonTier-SyslogAgent-1
04/30 17:55:23.000
12,663
MonTier-SyslogAgent-2
04/30 17:55:27.000
12,461
MonTier-SyslogAgent-3
04/30 17:56:22.000
7,735
MonTier-SyslogAgent-4
04/30 17:55:20.000
59
MonTier-SyslogAgent-5
04/30 17:55:20.000
59

WSM Agents

MonTier-WsmAgent-1
04/25 01:54:00.031
0
MonTier-WsmAgent-2
04/25 01:40:07.811
0

Resources Agents

Device Resources
04/30 17:56:02.000
39
Service Resources
04/25 01:14:09.000
0

5. Verify that Syslog and WS-M agents are Green.
   The Device Resources agent status should be green unless no monitored devices were added yet.

> The screenshot depicts a situation where both WS-M agents and Service Resources are down. This may point to a problem in the system or imply that services were stopped by the administrator.

Change Appliance Network Address

Appliance IP addresses are static by default. Hence, changing the IP address of the appliance is a 4-steps process.

1. Change the IP of a network device by editing the network configuration file. (E.g. for network card **eth0)**

   ```
   vi /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

   Change the values of **IPADDR** and **NETMASK** fields

   ifcfg-eth0

   ```
   #My IP description
   # IPv-4

   DEVICE="eth0"
   NM_CONTROLLED="yes"
   ONBOOT=yes
   HWADDR=00:ee:dd:cc:bb:aa
   TYPE=Ethernet
   BOOTPROTO=static
   NAME="System eth0"
   UUID=aaaabbbb-7777-8888-9999-aaaabbbbcccc
   IPADDR= 192.168.0.100
   NETMASK=255.255.255.0
   ```

   Use the command - *ip addr show* to see a device's IP address
2. When the appliance is moved to a different network subnet - Change the Default gateway

   ```
   vi /etc/sysconfig/network
   ```

   Change the value of the **GATEWAY** field in the file

   /etc/sysconfig/network

   ```
   NETWORKING=yes
   HOSTNAME=server1.example.com
   GATEWAY=192.168.0.1
   [...]
   ```

   Use the command - *ip route show* to see a device's IP address
3. Change DNS name (Optional step) - DNS can be added or changed in the file /etc/resolv.conf

```
vi /etc/resolv.conf
```

Change or add Domain Name Servers if required.

resolv.conf

```
[...]
nameserver 192.168.1.1
nameserver 192.168.1.2
[...]
```

4. Restart the network service

restart network services

```
service network restart
```

5. Edit the /etc/hosts file

   Change all the entries referring to the old IP address to use the new IP address. For example:

restart network services

```
192.168.65.175     montier-management
192.168.65.175     montier-syslog
192.168.65.175     montier-wsm
192.168.65.175     montier-ext-eth
```

   No need to change entries using the IP address 127.0.0.1

6. Stop and Start all system services.
7. In the web console navigate to **system nodes** and edit the IP address of the agents in your data node raw.
8. Re-configure syslog for the default domain on each monitored device (the Setup Syslog for device on the Device Management section)

Increase DPOD's Store Space

DPOD's Big Data Store is located on a dedicated hard drive. Occasionally, the disk space allocated for the Store needs to be increased. Reasons for that include an increase in TPS, or a requirement to retain history for longer periods of time.

The process to increase the disk space allocated to DPOD's Store entails the two stages detailed below:

- Increase DPOD's Store Space#Increase Data Disk.
- Increase DPOD's Store Space#Update Configuration File

Increase the Data Disk and File System

Physical Server

Use the server vendor's RAID management software to extend the existing RAID Disk (LUN) or add new RAID Disk (new LUN), in order to increase the data disk and file system sizes for the physical server.

Select the correct OS level configuration procedure below, based on whether you selected to extend or add a disk.

- Increase DPOD's Store Space#configure extended disk
- Increase DPOD's Store Space#configure new disk

Virtual appliance

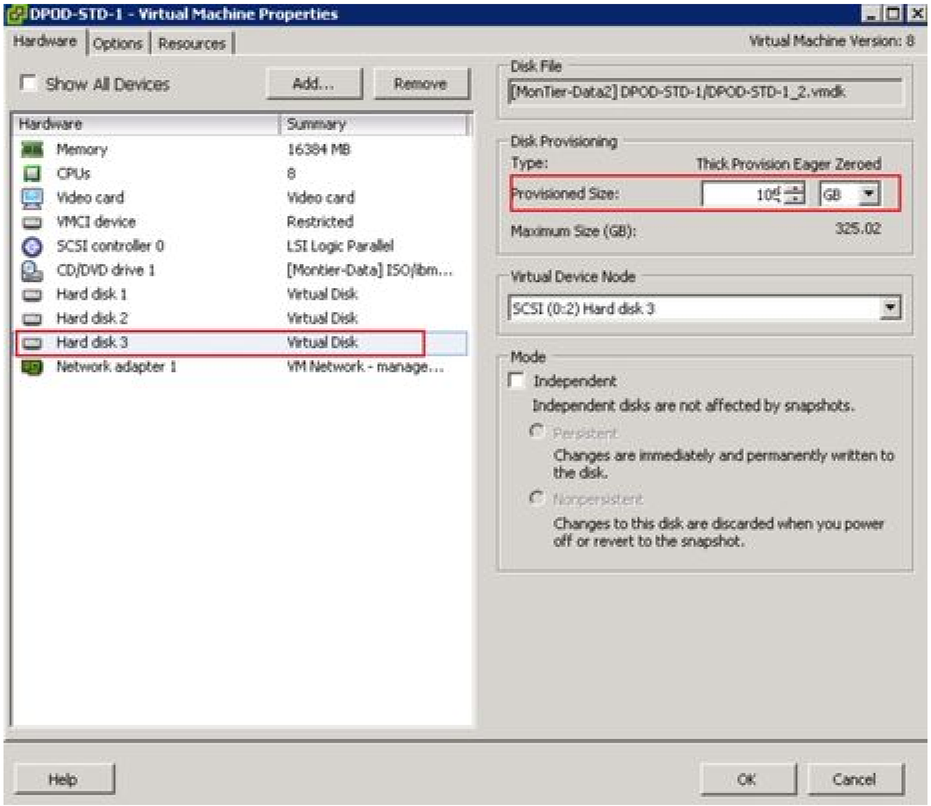
With a virtual deployment, there are two options available for increasing DPOD's Store disk space:

- Increase DPOD's Store Space#Extend an existing disk
- Increase DPOD's Store Space#Add a new disk

Extend the existing Virtual Disk

Use the VMware vSphere Client in order to edit the DPOD virtual machine

1. Stop the DPOD virtual machine.
2. Select **Edit virtual machine settings**
3. Select the 3rd hard drive (which is the data disk, as described in the Hardware and Software Requirements page).
4. Increase the **Provisioned size** of the hard drive and press OK.
5. Wait for the increase process to finish.
6. Start the DPOD virtual machine.



DPOD-STD-1 - Virtual Machine Properties

Virtual Machine Version: 8

☐ Show All Devices

Hardware	Summary
Memory	16384 MB
CPUs	8
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	[Montier-Data] ISO/ibm...
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Hard disk 3	Virtual Disk
Network adapter 1	VM Network - manage...

Disk File

[MonTier-Data2] DPOD-STD-1/DPOD-STD-1_2.vmdk

Disk Provisioning

Type: Thick Provision Eager Zeroed

Provisioned Size: 105 GB

Maximum Size (GB): 325.02

Virtual Device Node

SCSI (0:2) Hard disk 3

Mode

☐ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

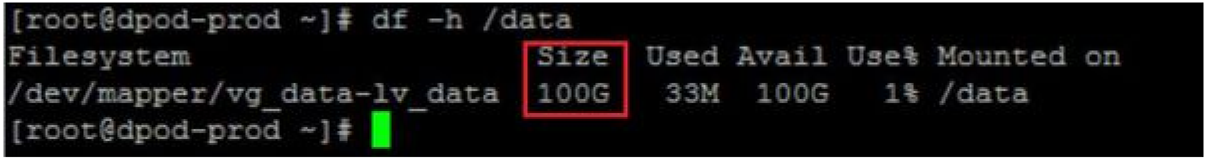
Changes to this disk are discarded when you power off or revert to the snapshot.

Configure the extended disk at the OS level

1. Verify the current size of mount point /data:

   ```
   df -h /data
   ```

   The system output should resemble the following:

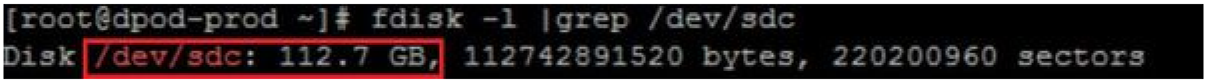
   

   ```
   [root@dpod-prod ~]# df -h /data
   Filesystem                    Size  Used Avail Use% Mounted on
   /dev/mapper/vg_data-lv_data   100G   33M  100G   1% /data
   [root@dpod-prod ~]#
   ```

2. Verify the new disk size:

   ```
   fdisk -l |grep /dev/sdc
   ```

   The system output should resemble the following:

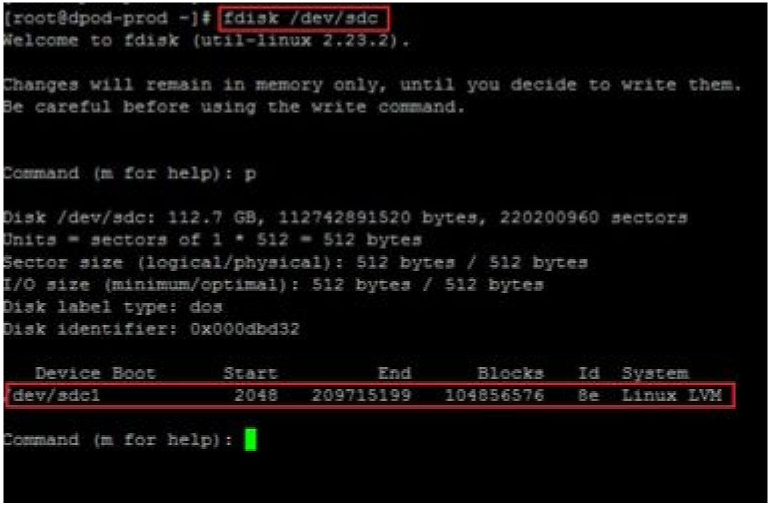
   ```
   [root@dpod-prod ~]# fdisk -l |grep /dev/sdc
   Disk /dev/sdc: 112.7 GB, 112742891520 bytes, 220200960 sectors
   ```

3. Use fdisk to create a new partition for the new size:

   ```
   fdisk /dev/sdc
   ```

   and perform the following steps:

   a. Press **p** to print the partition table to identify the number of partitions:

   ```
   [root@dpod-prod ~]# fdisk /dev/sdc
   Welcome to fdisk (util-linux 2.23.2).

   Changes will remain in memory only, until you decide to write them.
   Be careful before using the write command.


   Command (m for help): p

   Disk /dev/sdc: 112.7 GB, 112742891520 bytes, 220200960 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk label type: dos
   Disk identifier: 0x000dbd32

      Device Boot      Start         End      Blocks   Id  System
   /dev/sdc1            2048   209715199   104856576   8e  Linux LVM

   Command (m for help):
   ```

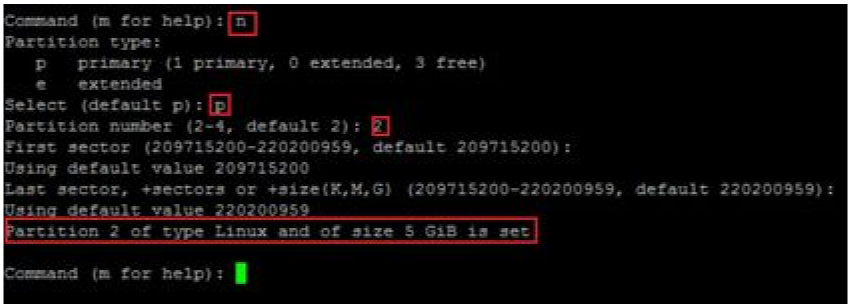
   If this is the first time the disk is extended, you should only see **sdc1**. If this is a subsequent extension - you will see additional sdcX listed (e.g. sdc2 for the second extension)

   b. Press **n** to create a new primary partition.

   c. Press **p** for primary.

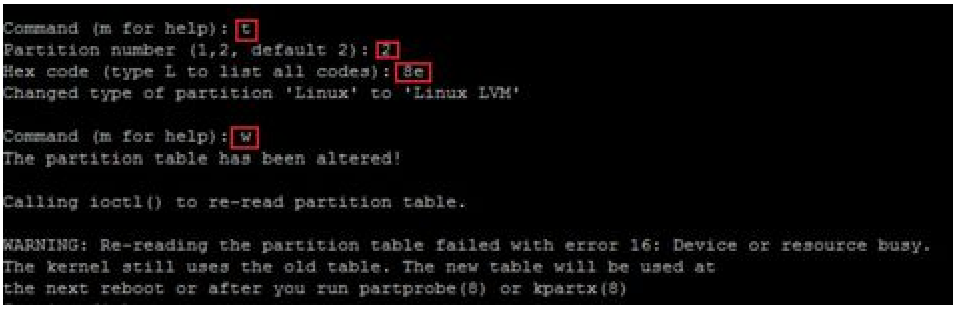
   d. When the system prompts for a partition number, enter the next number depending on the output of the partition table print. If this is the first extension and you see only one row of output - enter **2**. If this is the second disk extension then the partition number will be **3**, and so on.

   e. Press Enter twice



```
Command (m for help): n
Partition type:
   p   primary (1 primary, 0 extended, 3 free)
   e   extended
Select (default p): p
Partition number (2-4, default 2): 2
First sector (209715200-220200959, default 209715200):
Using default value 209715200
Last sector, +sectors or +size{K,M,G} (209715200-220200959, default 220200959):
Using default value 220200959
Partition 2 of type Linux and of size 5 GiB is set

Command (m for help):
```

f. Press **t** to change the system's partition ID.
g. Press **2** to select the newly created partition (Remember: if this is a subsequent disk extension - the number will be 3 or higher)
h. Type **8e** to change the Hex Code of the partition for Linux LVM.
i. Press **w** to write the changes to the partition table.



```
Command (m for help): t
Partition number (1,2, default 2): 2
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
```

> the following warning is valid, the system reboot will fix the issue :
> ***“WARNING: Re-reading the partition table failed with error 16: Device or resource busy.The kernel still uses the old table. The new table will be used at the next reboot or after you run partprobe(8) or kpartx(8)”***

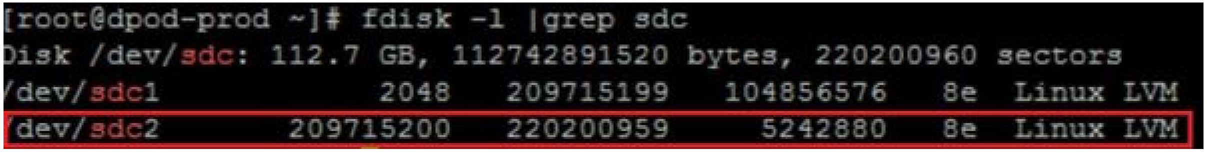
j. Reboot the system:

```
reboot
```

k. When the system is back up, ensure the new partition is available:

```
fdisk -l | grep /dev/sdc
```

The system output should resemble the following (note the new sdcX added)



```
[root@dpod-prod ~]# fdisk -l |grep sdc
Disk /dev/sdc: 112.7 GB, 112742891520 bytes, 220200960 sectors
/dev/sdc1            2048   209715199   104856576   8e  Linux LVM
/dev/sdc2       209715200   220200959     5242880   8e  Linux LVM
```

l. Stop the application by running app-util.sh and selecting option 2 (stop all)

> If the new partition is not sdc2, substitute sdc2 for the right qualifier in all the following commands

m. Create a new LVM Physical Volume (PV):

```
pvcreate /dev/sdc2
```

n. Extend the LVM Volume Group (VG):

```
vgextend vg_data /dev/sdc2
```

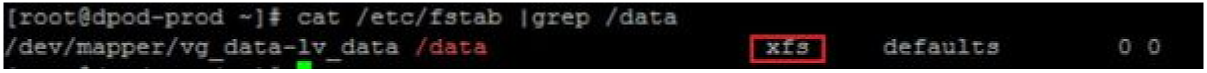
o. Extend the LVM Logical Volume (LV):

```
lvextend -l +100%FREE /dev/vg_data/lv_data
```

p. Identify the ***/data*** file system type (for CentOS 7.2 based appliances the type is xfs):

```
cat /etc/fstab |grep /data
```

The system output should resemble the following:



```
[root@dpod-prod ~]# cat /etc/fstab |grep /data
/dev/mapper/vg_data-lv_data /data                          xfs      defaults        0 0
```

q. Resize the file system. Select the correct command below for your file system type:

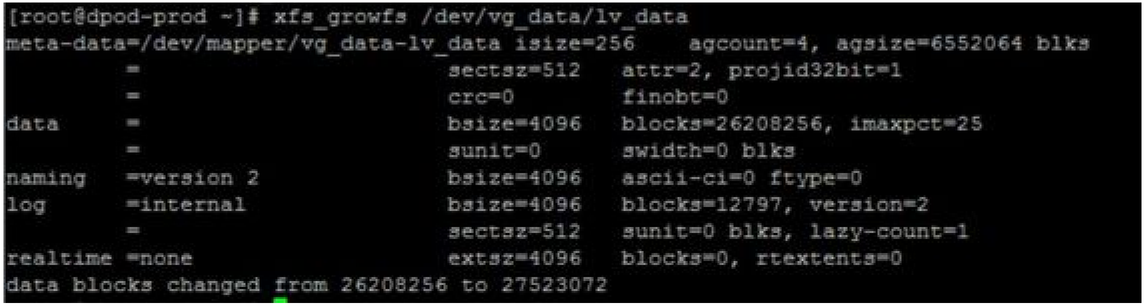
ext4

```
resize2fs /dev/vg_data/lv_data
```

xfs

```
xfs_growfs /dev/vg_data/lv_data
```

The system output should resemble the following:



```
[root@dpod-prod ~]# xfs_growfs /dev/vg_data/lv_data
meta-data=/dev/mapper/vg_data-lv_data isize=256    agcount=4, agsize=6552064 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=26208256, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=12797, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 26208256 to 27523072
```

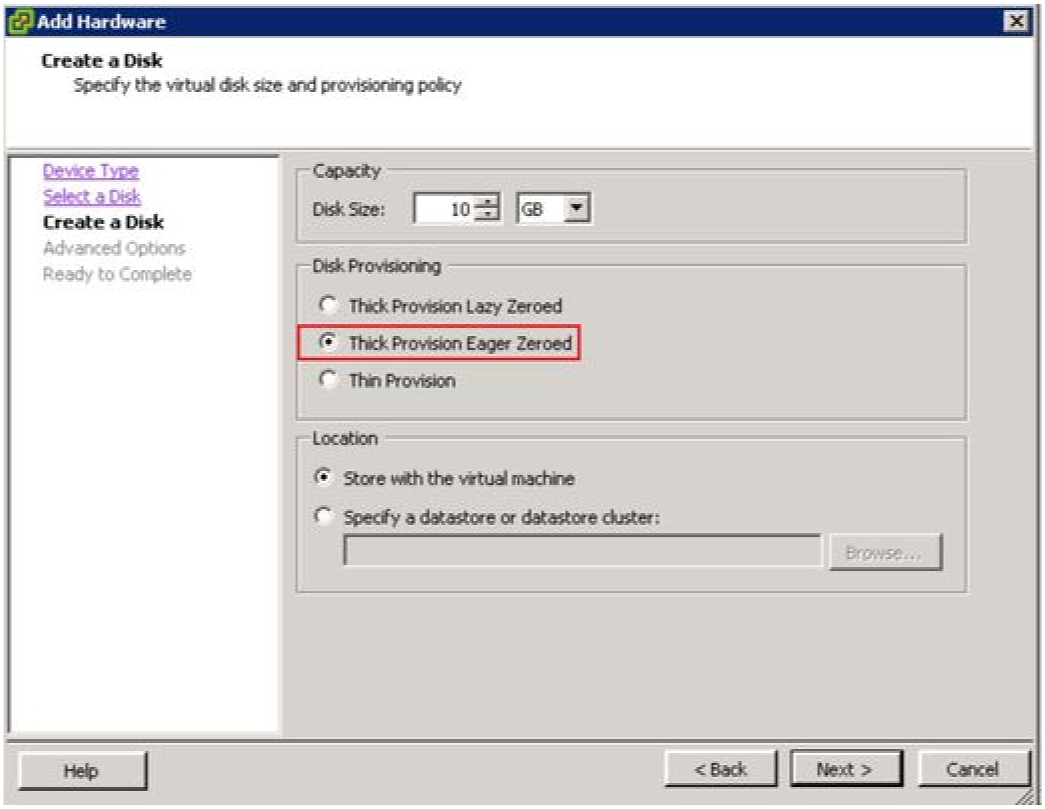
r. To display the new size of the ***/data*** mount point:

```
df -h /data
```

Add new virtual disk

Use the VMware vSphere Client in order to edit the DPODs virtual machine

1. Stop the DPOD virtual machine.
2. Select **Edit virtual machine settings**
3. Select **Add > Hard Drive**
4. Ensure to configure the new hard drive as **Thick Provision Eager Zeroed**
5. Wait for the increase process to finish.
6. Start the DPOD virtual machine



Add Hardware

Create a Disk

Specify the virtual disk size and provisioning policy

Capacity

Disk Size: 10 GB

Disk Provisioning

○ Thick Provision Lazy Zeroed

● Thick Provision Eager Zeroed

○ Thin Provision

Location

● Store with the virtual machine

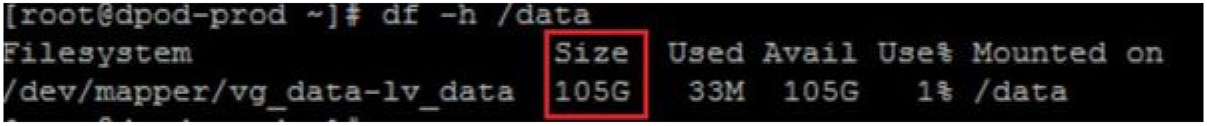
○ Specify a datastore or datastore cluster:

Configure the new disk at the OS Level

1. Verify the current size of the **/data** mount point:

   ```
   df -h /data
   ```

   The system output should resemble the following:

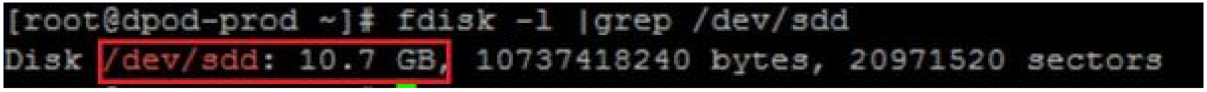
   

   ```
   [root@dpod-prod ~]# df -h /data
   Filesystem                    Size  Used Avail Use% Mounted on
   /dev/mapper/vg_data-lv_data   105G   33M  105G   1% /data
   ```

2. Verify the new disk size:

```
fdisk -l |grep /dev/sdd
```

The system output should resemble the following:

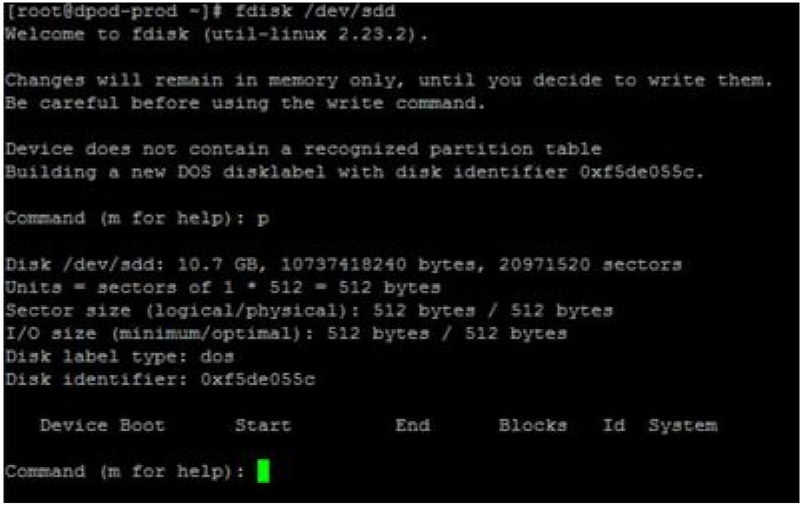


```
[root@dpod-prod ~]# fdisk -l |grep /dev/sdd
Disk /dev/sdd: 10.7 GB, 10737418240 bytes, 20971520 sectors
```

3. Create a new partition with the new size:

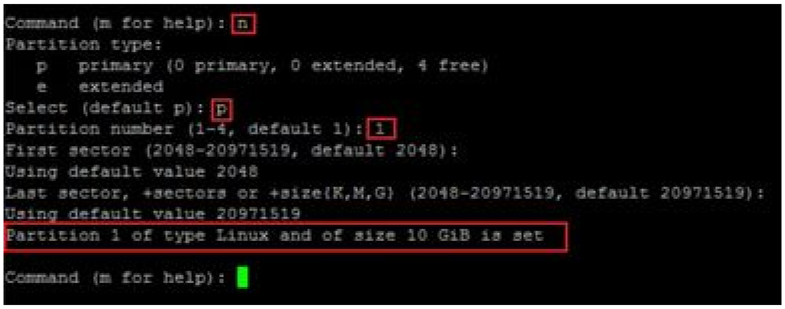
```
fdisk /dev/sdd
```

   a. Press **p** to print the partition table and ensure there are no existing partitions.



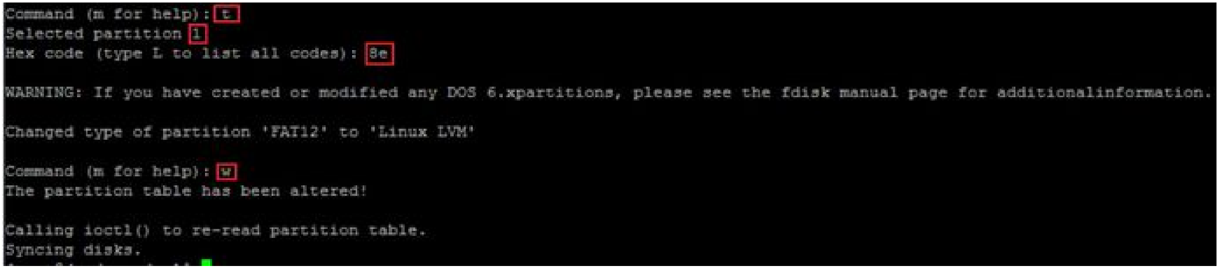
```
[root@dpod-prod ~]# fdisk /dev/sdd
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table
Building a new DOS disklabel with disk identifier 0xf5de055c.

Command (m for help): p

Disk /dev/sdd: 10.7 GB, 10737418240 bytes, 20971520 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0xf5de055c

   Device Boot      Start         End      Blocks   Id  System

Command (m for help):
```

   b. Press **n** to create a new primary partition.
   c. Press **p** for primary.
   d. Press **1** for the partition number
   e. Press Enter twice



```
Command (m for help): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519):
Using default value 20971519
Partition 1 of type Linux and of size 10 GiB is set

Command (m for help):
```

   f. Press **t** to change the system's partition ID.
   g. Type **8e** to change the Hex Code of the partition for Linux LVM.
   h. Press **w** to write the changes to the partition table.



```
Command (m for help): t
Selected partition 1
Hex code (type L to list all codes): 8e

WARNING: If you have created or modified any DOS 6.xpartitions, please see the fdisk manual page for additionalinformation.

Changed type of partition 'FAT12' to 'Linux LVM'

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

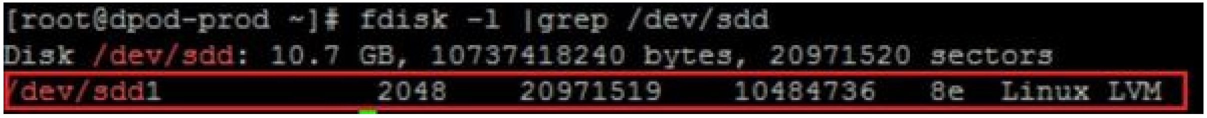
   i. Reboot the system:

```
reboot
```

j. When the system is back up, ensure the new partition is created:

```
fdisk -l |grep /dev/sdd
```

The system output should resemble the following:



```
[root@dpod-prod ~]# fdisk -l |grep /dev/sdd
Disk /dev/sdd: 10.7 GB, 10737418240 bytes, 20971520 sectors
/dev/sdd1              2048    20971519    10484736   8e  Linux LVM
```

k. Stop the application by running app-util.sh and selecting option 2 (stop all)
l. Create a new LVM Physical Volume (PV):

```
pvcreate /dev/sdd1
```

m. Extend the LVM Volume Group (VG):

```
vgextend vg_data /dev/sdd1
```

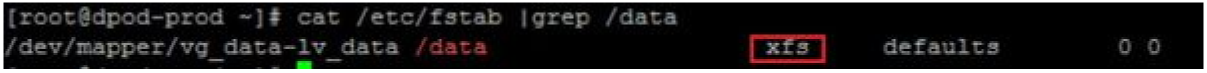
n. Extend the LVM logical volume (LV):

```
lvextend -l +100%FREE /dev/vg_data/lv_data
```

o. Identify the **/data** file system type (for CentOS 7.2 based appliances the type is xfs):

```
cat /etc/fstab |grep /data
```

The system output should resemble the following:



```
[root@dpod-prod ~]# cat /etc/fstab |grep /data
/dev/mapper/vg_data-lv_data /data                    xfs     defaults        0 0
```

p. Resize the file system. Select the correct command below for your file system type:

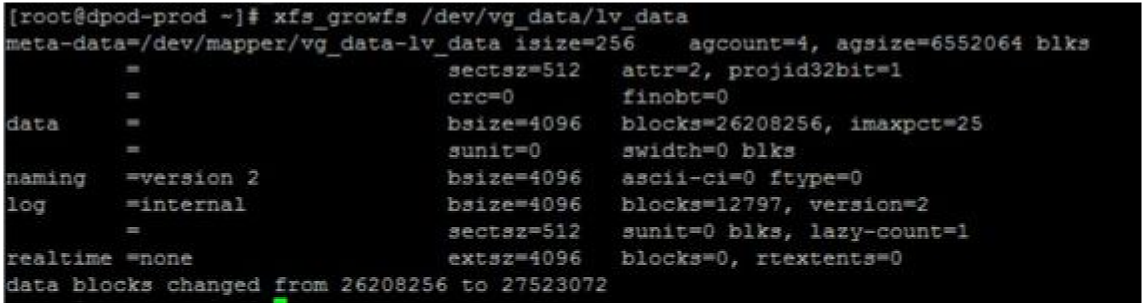
ext4

```
resize2fs /dev/vg_data/lv_data
```

xfs

```
xfs_growfs /dev/vg_data/lv_data
```

The system output should resemble the following:

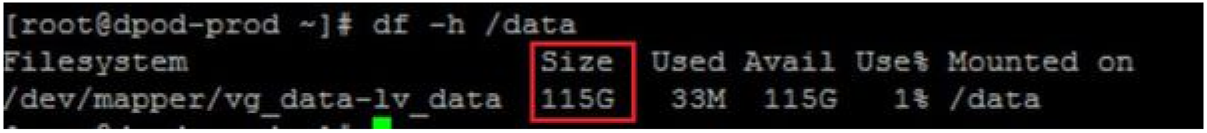


```
[root@dpod-prod ~]# xfs_growfs /dev/vg_data/lv_data
meta-data=/dev/mapper/vg_data-lv_data isize=256    agcount=4, agsize=6552064 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=26208256, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal               bsize=4096   blocks=12797, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
data blocks changed from 26208256 to 27523072
```

q. To display the new size of the **/data** mount point:

```
df -h /data
```

The system output should resemble the following:



```
[root@dpod-prod ~]# df -h /data
Filesystem                   Size  Used Avail Use% Mounted on
/dev/mapper/vg_data-lv_data  115G   33M  115G   1% /data
```

Update the Store Configuration File

Starting with v1.0.4, DPOD is shipped with a script that performs all the necessary steps to update the Store configuration file.

You may use this script by running:

```
/app/scripts/update_store_allocation.sh
```

The script is available on DPOD v1.0.4 and above. If you are using earlier version please contact DPOD support and the script will be provided.

When the script has completed, restart the application by running app-util.sh and selecting option 1 (start all)

INCREASE STORAGE FOR INDEX SETS

> This procedure should be performed only after consulting with product support team

Depending on your data retention configuration, you may find that you need to increase the amount of data DPOD is able to store. In those circumstances, you will need to perform the steps below.

1. Ensure the disks mounted to the /data path have enough free space to accommodate your needs.
   The maximum increase amount (MAX_INC_IX_SIZE) is calculated as the total free space of /data - 15GB. The information regarding /data storage can be found on the OS screen.
2. To calculate the correct Index set increase, consult these parameters (available on the Store screen)
   a. The number of days currently stored: Index Sets table (this is Newest Document Time - Oldest Document Time)
   b. The amount of storage you are using: Index Sets table (size)
   c. the number of indexes allocated: Index Sets table (Indices count)
3. As a general rule of thumb, increase the Index Sets size together with their number. Ideally each index will be large enough to contain information for 1.5-2 days. MAX_INC_IX_NUMBER
4. Additionally, increase memory by 32-96GB for each additional 1TB Data stored. The exact value depends on data variance and acceptable response time from the queries.
5. Once you have calculated values for MAX_INC_IX_NUMBER and MAX_INC_IX_SIZE , go to file /app/hk_retention/MonTier-HK-ESRetention/conf/MonTierHousekeeping.conf
6. edit the file. Change the number of indexes with MAX_INC_IX_NUMBER and the total storage allocated with MAX_INC_IX_SIZE.
7. for example, to extend the wdp-syslog - change the following properties:

```
# WDP Syslog tran index set number of indices, usually 20
elasticsearch.index_set.wdp-syslog-tran.indices_count=<MAX_INC_IX_NUMBER>

# WDP Syslog tran index set max size - NOTE the G for GB at the end.
elasticsearch.index_set.wdp-syslog-tran.max_size=<MAX_INC_IX_SIZE>G
```

Changing Agents TCP port

DPOD's agents (both Syslog and WS-M) listen on predefined TCP ports:

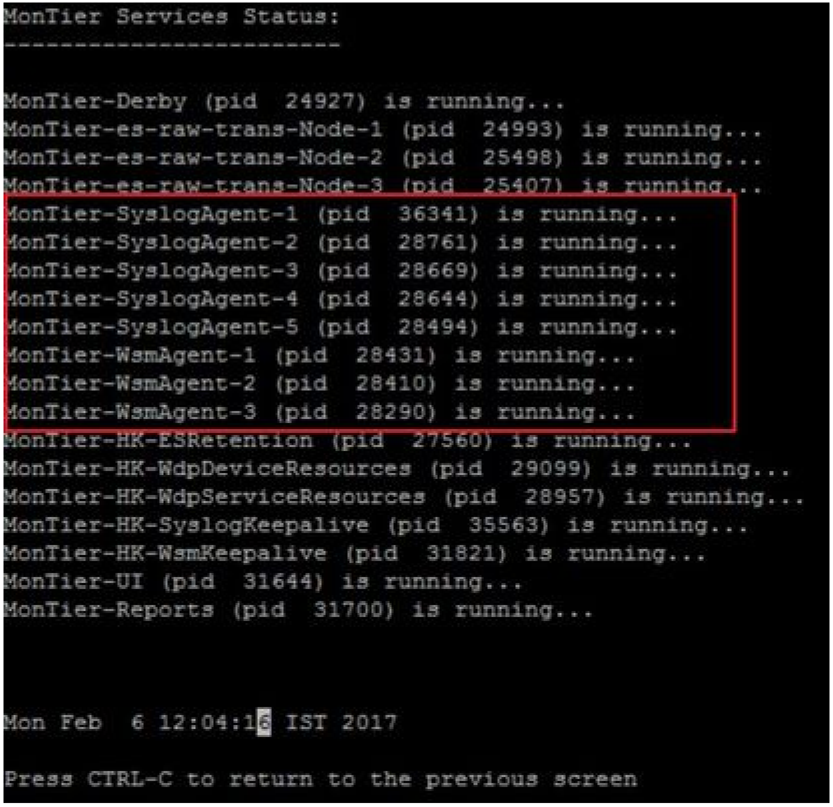
Syslog agents - 60000-60009

WS-M agents - 60020-60029

In order to change these default ports, please use the following procedure.

Changing the agent’s configuration

1. Identify your existing agents by using the CLI Admin utility. From a console / ssh session, invoke the command app-util.sh and select option 3 (check status). A list of DPOD’s services will be displayed including the Syslog and WS-M agents.
For example:



```
MonTier Services Status:
------------------------

MonTier-Derby (pid  24927) is running...
MonTier-es-raw-trans-Node-1 (pid  24993) is running...
MonTier-es-raw-trans-Node-2 (pid  25498) is running...
MonTier-es-raw-trans-Node-3 (pid  25407) is running...
MonTier-SyslogAgent-1 (pid  36341) is running...
MonTier-SyslogAgent-2 (pid  28761) is running...
MonTier-SyslogAgent-3 (pid  28669) is running...
MonTier-SyslogAgent-4 (pid  28644) is running...
MonTier-SyslogAgent-5 (pid  28494) is running...
MonTier-WsmAgent-1 (pid  28431) is running...
MonTier-WsmAgent-2 (pid  28410) is running...
MonTier-WsmAgent-3 (pid  28290) is running...
MonTier-HK-ESRetention (pid  27560) is running...
MonTier-HK-WdpDeviceResources (pid  29099) is running...
MonTier-HK-WdpServiceResources (pid  28957) is running...
MonTier-HK-SyslogKeepalive (pid  35563) is running...
MonTier-HK-WsmKeepalive (pid  31821) is running...
MonTier-UI (pid  31644) is running...
MonTier-Reports (pid  31700) is running...



Mon Feb  6 12:04:16 IST 2017

Press CTRL-C to return to the previous screen
```

2. Stop the agents that are about to be changed using the CLI Admin utility.

3. Change the agents' listening port. From a console / ssh session invoke the command:

```
/app/scripts/change_agent_config.sh -t|--agent-type <syslog | wsm>
-n|--agent-number <number> -p|--agent-port <TCP port>
```

> The script is available in DPOD v1.0.4.0 and above. For earlier versions please contact DPOD support.

Operation	Purpose
-t, --agent-type	The agent type: Syslog or WS-M
-n, --agent-number	The agent number, for example: MonTier-SyslogAgent-3 is syslog agent number 3
-p, --agent-port	The new TCP port for the agent

For example, the following command will change the listening port for syslog agent number 1 to TCP port 60000:

```
/app/scripts/change_agent_config.sh -t syslog -n 1 -p 60000
```

4. Restart (stop and start) the agents internal keepalive service (hk_keepalive) using the CLI Admin utility.
5. Start the agents' services (Syslog / WS-M) using the CLI Admin utility.

Changing firewall rules

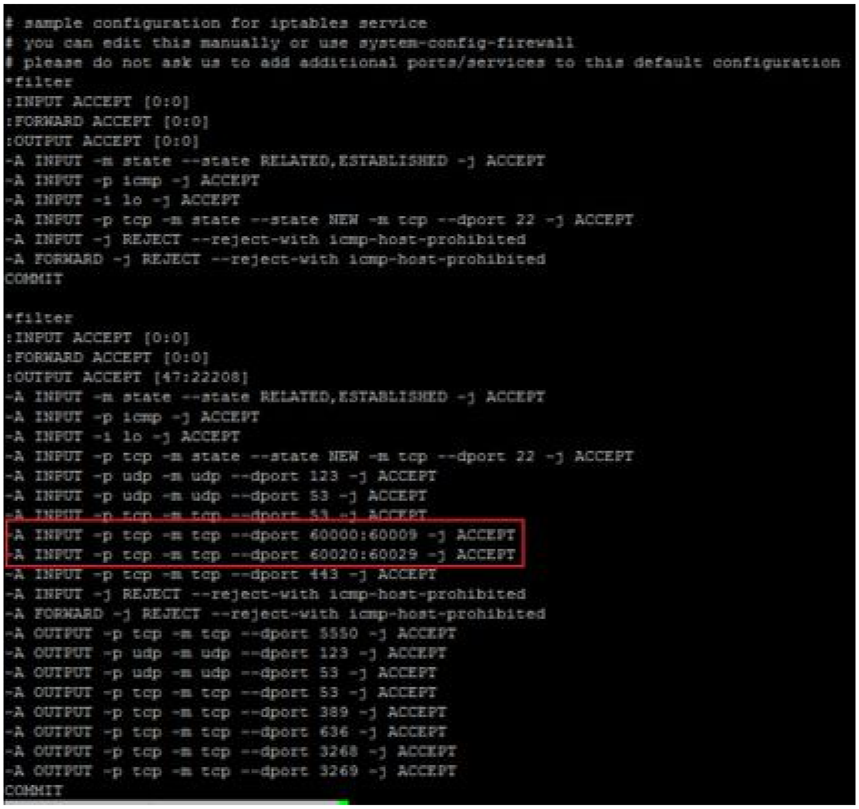
1. Update DPOD's firewall service (iptables) rules to accepts network traffic using the new TCP ports.

> It is highly recommend to backup the configuration file before editing it (make a copy of the file).

2. Edit the iptables configuration file:

```
vi /etc/sysconfig/iptables
```

The relevant rules for the agent network traffic are marked. Alter the rules corresponding to the new agents' ports (for example change ports 60000:60009 to 10000:10009):



```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# please do not ask us to add additional ports/services to this default configuration
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [47:22208]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 60000:60009 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 60020:60029 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -p tcp -m tcp --dport 5550 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 389 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 636 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 3268 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 3269 -j ACCEPT
COMMIT
```

3. Restart iptables service for the new rules to take effect:

```
service iptables restart
```

Reconfigure DataPower to work with the new agents' ports

> This step is required only if changes were made to agents that are already receiving network traffic from DataPower devices.

1. Make sure DataPower has network connectivity to the agents using the new agents TCP ports. See Network Preparation.
2. Redeploy DPOD Syslog log targets to DataPower ("Setup Syslog for the New Monitored Devices" and "Syslog Setup for all Domains")

Adding Second Network Interface to DPOD

DPOD can be configured with two network interfaces:

1. First interface - for accessing DPOD's Web Console via web browser and DPOD's CLI via SSH.
2. Second interface - for communicating with the monitored devices.

> The second network interface cannot share the same class C network as the first network interface (for example, the two interfaces cannot have IP addresses on the subnet 192.169.10.x).

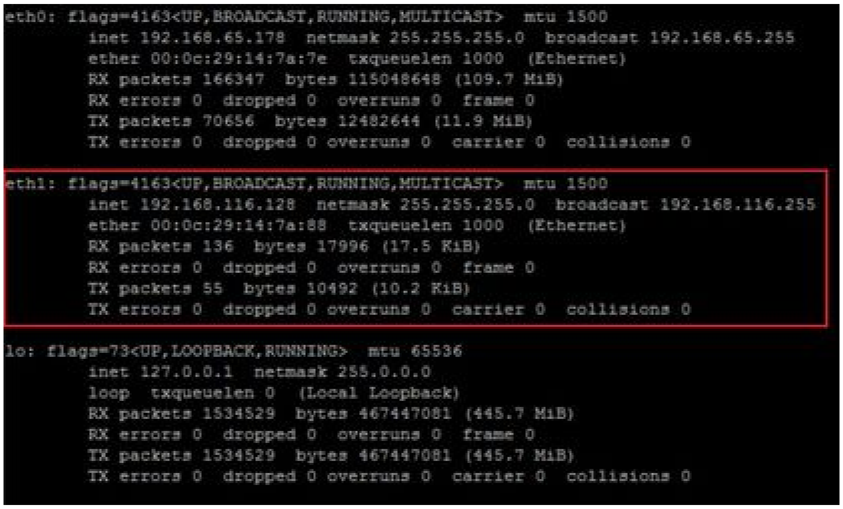
CONNECT THE SECOND NETWORK INTERFACE TO THE SERVER

Use your system administrator assistance to add a second network interface to your virtual machine or physical server.

In some cases, there will be a need to restart the server before the new network will be available.

After the server restarts, the operating system will automatically configure the new network interface using DHCP.

Log in to DPOD's Console or CLI via SSH with the user "root" and type the command "ifconfig". The command output should be similar to the following screenshot:



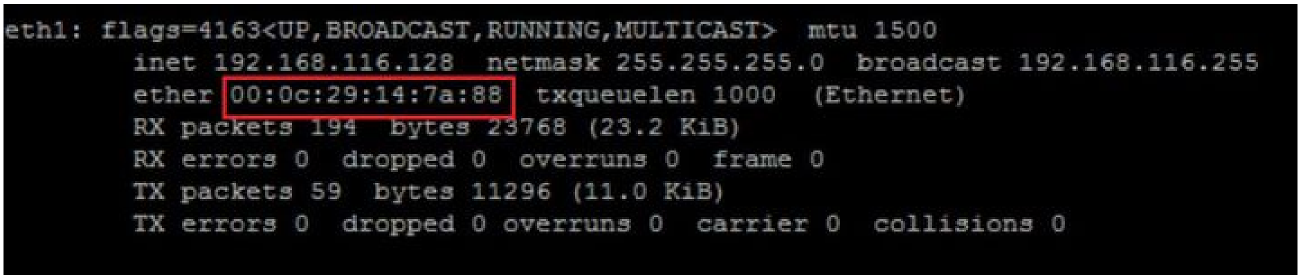
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.65.178  netmask 255.255.255.0  broadcast 192.168.65.255
        ether 00:0c:29:14:7a:7e  txqueuelen 1000  (Ethernet)
        RX packets 166347  bytes 115048648 (109.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 70656  bytes 12482644 (11.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.116.128  netmask 255.255.255.0  broadcast 192.168.116.255
        ether 00:0c:29:14:7a:88  txqueuelen 1000  (Ethernet)
        RX packets 136  bytes 17996 (17.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 55  bytes 10492 (10.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 0  (Local Loopback)
        RX packets 1534529  bytes 467447081 (445.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1534529  bytes 467447081 (445.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The new network interface should be displayed as "eth1".

> On a Non-Appliance installation when customer provides pre-installed server, the network interfaces names might be different (the network interface naming depends on the operating system configuration).

CONFIGURE THE NEW NETWORK INTERFACE

1. Copy the network interface MAC address as displayed in the "ifconfig" command output after the attribute "ether":



```
eth1:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.116.128  netmask 255.255.255.0  broadcast 192.168.116.255
        ether 00:0c:29:14:7a:88  txqueuelen 1000  (Ethernet)
        RX packets 194  bytes 23768  (23.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59  bytes 11296 (11.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Change directory to /etc/sysconfig/network-scripts:

```
cd /etc/sysconfig/network-scripts
```

3. Duplicate eth0 (first network interface) network interface configuration file for the new network interface file (eth1):

```
cp ifcfg-eth0 ifcfg-eth1
```

4. Edit the new file (ifcfg-eth1) and alter the following attributes based on the new network interface properties

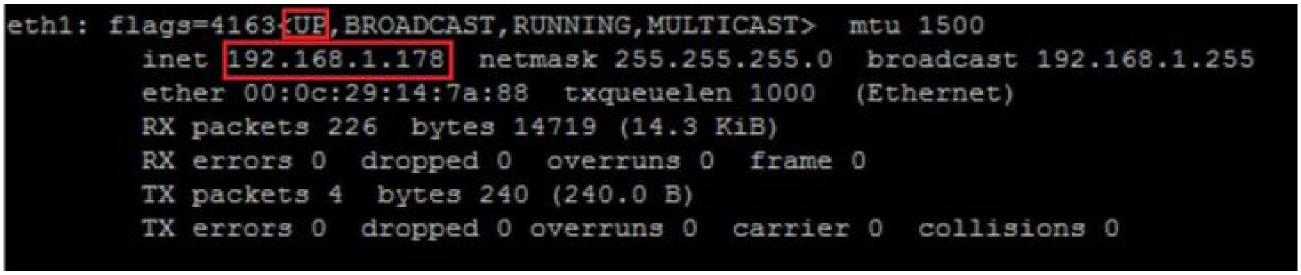
```
DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
NM_CONTROLLED=no
HWADDR=00:0c:29:14:7a:88
IPADDR=192.168.1.178
NETMASK=255.255.255.0
USERCTL=no
DNS1=8.8.8.8
DNS2=8.8.4.4
IFCONFIG_OPTS="txqueuelen 10000"
```

DEVICE   : The network interface device name should be eth1
HWADDR : The network interface MAC address as displayed at section 1
NETMASK : The network mask based on the new interface properties (the network administrator should supply this information)

5. Restart the network service by entering the following command:

```
service network restart

The output should be:
Restarting network (via systemctl):                        [  OK  ]
```

6. Use the command "ifconfig" to make sure the new network interface is up and configured with the correct IP address:



```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.178  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:14:7a:88  txqueuelen 1000  (Ethernet)
        RX packets 226  bytes 14719 (14.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

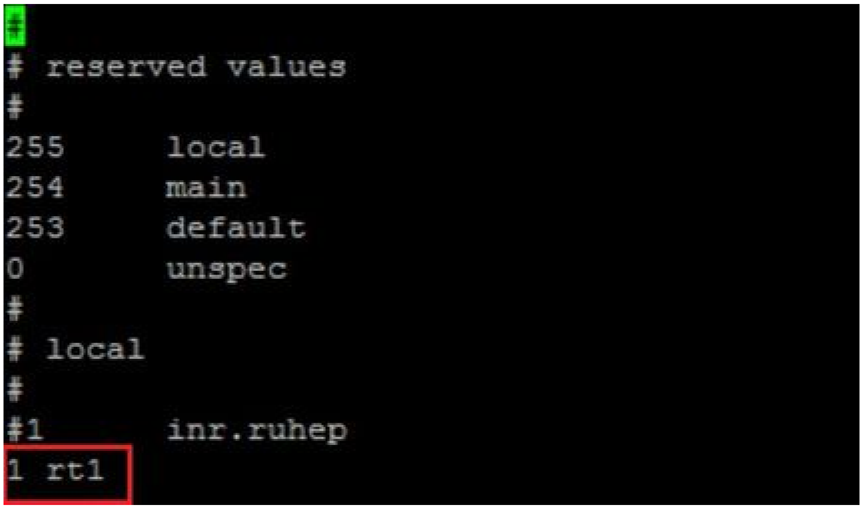
If the new IP address is not displayed restart the server.

CONFIGURE ROUTING

In order to support the second network interface, a new routing table and routing rules should be defined.

Create New Routing Table

1. Edit the file /etc/iproute2/rt_tables and add new routing table entry with id "1" named "rt1":



```
#
# reserved values
#
255     local
254     main
253     default
0       unspec
#
# local
#
#1      inr.ruhep
1 rt1
```

2. In order to add new routing entry to the new routing table use the "ip route" command.
   This command will add new temporary entry to the routing table.

3. Add a default gateway entry (should be executed only once)

```
ip route add default via <interface default gateway> dev <interface
name> table <routing table name>
```

   Example: For adding the default gateway 192.168.1.1 to interface eth1:

```
ip route add default via 192.168.1.1 dev eth1 table rt1
```

   Adding a default gateway to a network interface should be executed only once.

4. Add a routing entry (should be executed as needed for every monitored device):

```
ip route add <destinamtion ip address or subnet> dev <interface
name> table <routing table name>
```

   Example: For adding the route entry to subnet 192.168.1.x to interface eth1

```
ip route add 192.168.1.0/24 dev eth1 table rt1
```

> Adding specific routing entry should be executed as needed for every monitored device

5. In order to make these entries permanent edit the file /etc/sysconfig/network-scripts/route-<interface name> and add the following:

```
default via <interface default gateway> dev <interface name> table
<routing table name>
<destinamtion ip address or subnet> dev <interface name> table
<routing table name>
```

For example: Create new permanent routing file for interface eth1 and add the entries used at previous examples:

```
default via 192.168.1.1 dev eth1 table rt1
192.168.1.0/24 dev eth1 table rt1
```

6. To confirm that the new routing table includes the new routing entries use the following command to display the content of the table:

```
ip route show tab <routing table name>
```

For example: To display the content of table rt1:

```
ip route show tab rt1

The output should be:
default via 192.168.1.1 dev eth1
192.168.1.0/24 dev eth1  scope link
```

Create a New Routing Rule

The routing rule instructs the operating system when to use the new routing table.

1. In order to add a new routing rule entry to the new routing table use the "ip rule" command.
   This command will add a new temporary rule entry.

```
ip rule add from <source ip address or subnet> table <routing table
name>
ip rule add to <destination ip address or subnet> table <routing
table name>
```

For example: The routing rule for monitored device 192.168.1.120 are

```
ip rule add from 192.168.1.120/32 table rt1
ip rule add to 192.168.1.120/32 table rt1
```

The specific IP address can be replaced with subnet if subnet rule is appropriate: 192.168.1.0/24

2. In order to make these entries permanent edit the file /etc/sysconfig/network-scripts/rule-<interface name> and add the following:

```
from <source ip address or subnet> table <routing table name>
to <destination ip address or subnet> table <routing table name>
```

For example: The routing rule for monitored device 192.168.1.120 are

```
from 192.168.1.120/32 table rt1
to 192.168.1.120/32 table rt1
```

3. To confirm that the new routing rules entries added use the following command to display them:

```
ip rule show

The output should include the following lines:
32764:  from all to 192.168.1.120 lookup rt1
32765:  from 192.168.1.120 lookup rt1
```

CONFIRM THE NEW CONFIGURATION

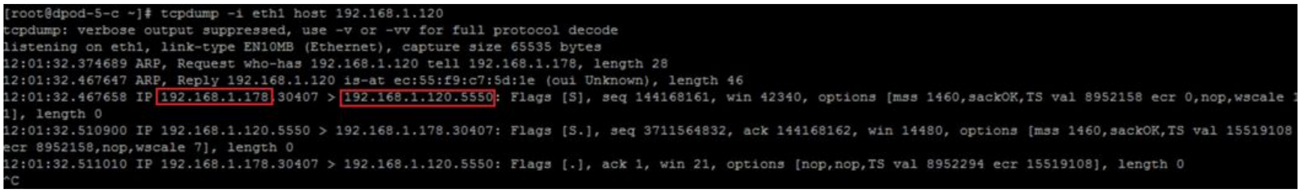
1. Restart the server.
2. After the server is up again login via SSH.
   Use the "ip route show tab" command and the "ip rule show" command make sure the routing entries and the routing rule persists after the restart.
3. Confirm the needed network connectivity to the monitored device:
   Open new CLI session via SSH and start capture network traffic passing through eth1 to the wanted monitored device.
   The following command will capture network traffic to 192.168.1.120:

```
tcpdump -i eth1 host 192.168.1.120
```

On the second SSH session run telnet command to test connectivity to the monitored device using port 5550 (XML Management Interface Port):

```
telnet 192.168.1.120 5550
```

The output of the tcpdump command should look similar to the following:
The source of the tcp connection is the new eth1 ip address and the destination is the monitored device ip address:



```
[root@dpod-5-c ~]# tcpdump -i eth1 host 192.168.1.120
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
12:01:32.374689 ARP, Request who-has 192.168.1.120 tell 192.168.1.178, length 28
12:01:32.467647 ARP, Reply 192.168.1.120 is-at ec:55:f9:c7:5d:1e (oui Unknown), length 46
12:01:32.467658 IP 192.168.1.178.30407 > 192.168.1.120.5550: Flags [S], seq 144168161, win 42340, options [mss 1460,sackOK,TS val 8952158 ecr 0,nop,wscale
1], length 0
12:01:32.510900 IP 192.168.1.120.5550 > 192.168.1.178.30407: Flags [S.], seq 3711564832, ack 144168162, win 14480, options [mss 1460,sackOK,TS val 15519108
ecr 8952158,nop,wscale 7], length 0
12:01:32.511010 IP 192.168.1.178.30407 > 192.168.1.120.5550: Flags [.], ack 1, win 21, options [nop,nop,TS val 8952294 ecr 15519108], length 0
^C
```

CONFIGURE DPOD FOR THE NEW NETWORK INTERFACE

After the new network interface is configured correctly, DPOD configuration needs to change to use the new interface.

Change DPOD Configuration

1. Edit the file /etc/hosts and alter the following entries to point to the new IP address.
   For example, these are the entries for the new IP address 192.168.1.178:

```
192.168.1.178     montier-syslog
192.168.1.178     montier-wsm
```

2. Restart the application using the CLI Admin Menu.

Re-configure Syslog and WS-M

After DPOD was configured to use the new IP address, the monitored devices need to be re-configured to communicate with DPOD via the new address.

In order to re-configure the monitored devices, please follow the instructions under "Adding Monitored Devices" - sub items "Setup Syslog for the New Monitored Device" and "WS-M setup for device".

Change sampling interval intervals

System Directories structure

Directory Name	Description
/app	Include the system's components configuration and run-time. Every component has dedicated directory. examples : /app/ui - The Web Console application server /app/reports - The reports application server /app/elasticsearch_nodes - The Store nodes /app/flume - The system agents (wsm agents, syslog agents)
/data	Include the system data. Examples: /data/es-raw-trans - The store nodes data files /data/reports - The generated reports files (when the system is configured to generate reports to files)
/logs	Include the system's components logs. Every component has dedicated directory. Examples: /logs/ui - The Web Console logs. /logs/es-raw-trans - The Store nodes logs
/installs	Includes the system installation artifacts. Most of the installation artifacts plays role only during system installation with the following exceptions: /installs/logs - The system installation logs /installs/update/fix - The directory for system updates staging. includes the directory /installs/update/fix/backups for the pre-update system backup. /installs/system-backup - The system backup directory
/shared	Includes data that is shared between the system components.

DevOps Portal Setup and Security

- DevOps Portal Setup and Customization
- DevOps Portal Security

DevOps Portal Setup and Customization

Before you can use certain features of the DevOps portal, you will need the following setup/configuration:

REMOTE OR LOCAL WSDL VALIDATION/PROMOTION

1. If you wish to use Remote or Local WSDL validation or promotion - create a temporary domain(s) for DPOD operations
   DPOD will create temporary services on this domain in order to validate the service WSDL and may upload files to the local filesystem.
   a. Per-device temporary domain:
   From Monitored Devicesmonitored deviceSettings Tab, choose a temporary domain
   The temporary domain needs to be accessible to this device, you may choose the same temporary domain for multiple devices

   b. Default temporary domain for all devices that don't have per-device setup
   Enter the temporary domain's device name in DPOD's system parameter (see "DevOps Portal Parameters" section under system parameters)
   Enter the temporary domain's name in DPOD's system parameter (see "DevOps Portal Parameters" section under system parameters)

   > It is the Gateway admin's responsibility to clear the temporary domain's content and/or services.
   > DPOD does not clear the domain's content.
   > Once DPOD finished validating or promoting a service, the temporary service and its files are no longer required and can be safely deleted.

   > For remote WSDL validation or promotion - the temporary domain should have access to the remote WSDL address.
   > Read Remote WSDL Validation and Promotion to learn more about how the remote WSDL validation is performed

2. If you wish to use Local WSDL validation or promotion you will need to use two custom Python scripts,
   a. a script to analyze the WSDL/XSD files
   b. a script to replace references in the WSDL/XSD files.
   see DevOps Services Portal's User Scripts for more information about the script specifications.
   Once you uploaded the scripts to DPOD, you will need to setup their path and names in DPOD's system parameters so DPOD can use them (see "DevOps Portal Parameters" section under system parameters)
   c. You can limit the maximum WSDL and XSD file sizes that users are allowed to upload (see "DevOps Portal Parameters" section under system parameters)
3. After setting up the monitored devices, you can setup DNS translations for the DevOps services list page

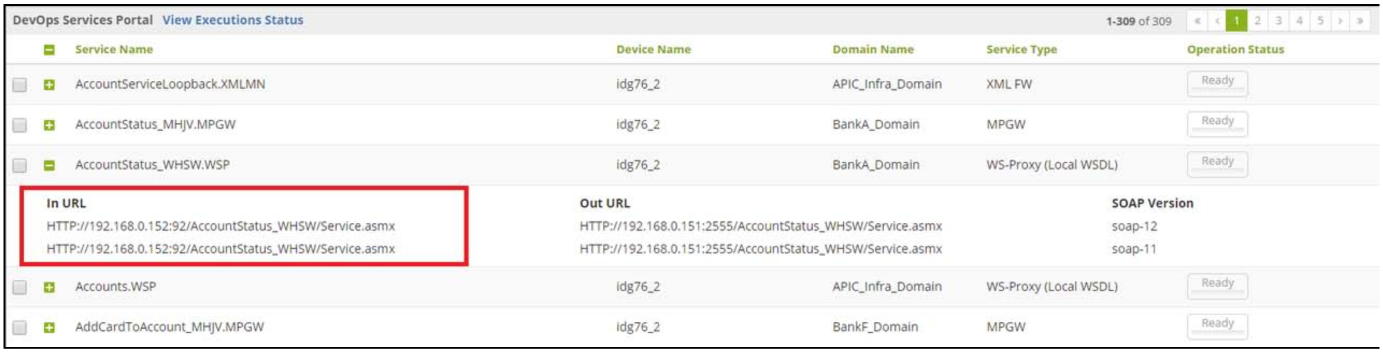
IMPORT SERVICE

1. You can set whether a deployment policy is mandatory for imports - see "Deployment Policy is Mandatory for Import Service" in system parameters for more info (refresh your browser page after changing the system parameter value)
2. The users will be promoted to select a deployment policy from a list of deployment policies that were pre-loaded to a specific folder in DPOD's
   Set the folder from the "Import Service Deployment Policies Path" parameter in system parameters and upload files to the DPOD server using any file-transfer program (refresh your browser page after changing the system parameter value)
3. You can set a size limit to the uploaded import files, the default value is 10MB, see "Import Service Max Upload File Size in KB" in system parameters for more info
4. The Import service process includes two custom user scripts,
   The first script gets the user deployment policy's selection, and can override or change it.
   The second script performs validations on the export file, before the import begins.
   The location of the scripts is set in system parameters, default scripts and setup is supplied, you may replace or edit the initial scripts.
   see DevOps Services Portal's User Scripts for more information about the script specifications.

DevOps Portal Services List DNS Translation

Use the DNS translation table to change the contents of the "In URL" field in the DevOps Portal Services List

For example, before the DNS translation:



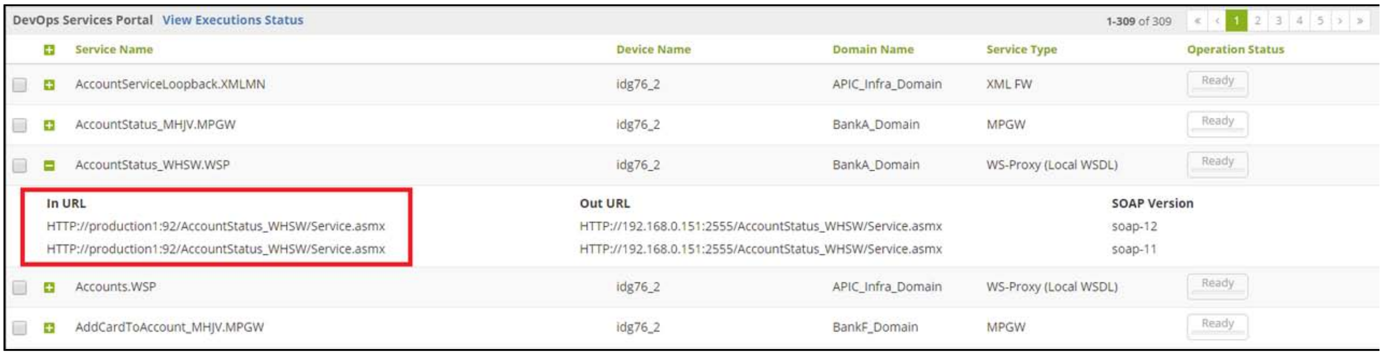
DevOps Services Portal View Executions Status 1-309 of 309

	Service Name	Device Name	Domain Name	Service Type	Operation Status
□	AccountServiceLoopback.XMLMN	idg76_2	APIC_Infra_Domain	XML FW	Ready
□	AccountStatus_MHJV.MPGW	idg76_2	BankA_Domain	MPGW	Ready
□	AccountStatus_WHSW.WSP	idg76_2	BankA_Domain	WS-Proxy (Local WSDL)	Ready

In URL	Out URL	SOAP Version
HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-12
HTTP://192.168.0.152:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-11

	Service Name	Device Name	Domain Name	Service Type	Operation Status
□	Accounts.WSP	idg76_2	APIC_Infra_Domain	WS-Proxy (Local WSDL)	Ready
□	AddCardToAccount_MHJV.MPGW	idg76_2	BankF_Domain	MPGW	Ready

After the translation:



DevOps Services Portal View Executions Status 1-309 of 309

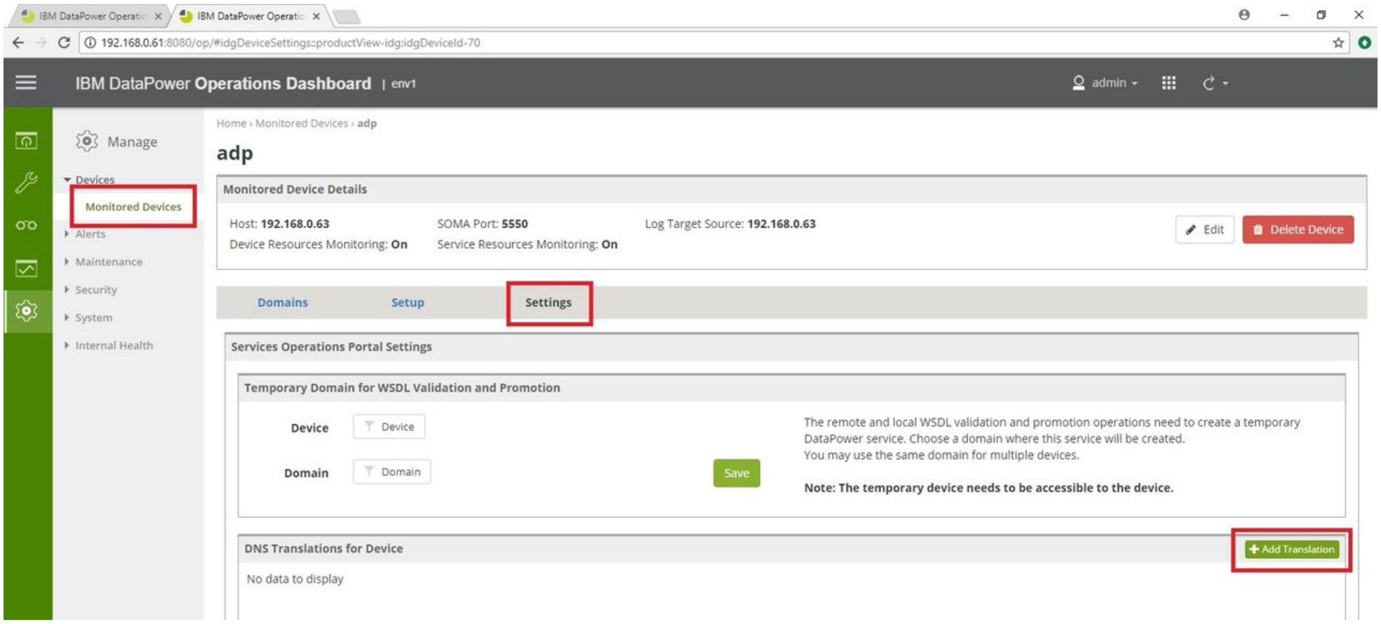
	Service Name	Device Name	Domain Name	Service Type	Operation Status
□	AccountServiceLoopback.XMLMN	idg76_2	APIC_Infra_Domain	XML FW	Ready
□	AccountStatus_MHJV.MPGW	idg76_2	BankA_Domain	MPGW	Ready
□	AccountStatus_WHSW.WSP	idg76_2	BankA_Domain	WS-Proxy (Local WSDL)	Ready

In URL	Out URL	SOAP Version
HTTP://production1:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-12
HTTP://production1:92/AccountStatus_WHSW/Service.asmx	HTTP://192.168.0.151:2555/AccountStatus_WHSW/Service.asmx	soap-11

	Service Name	Device Name	Domain Name	Service Type	Operation Status
□	Accounts.WSP	idg76_2	APIC_Infra_Domain	WS-Proxy (Local WSDL)	Ready
□	AddCardToAccount_MHJV.MPGW	idg76_2	BankF_Domain	MPGW	Ready

Entering a New Translation

From the **[ManageMonitored Devicesmonitored device]** page, click on the desired device, and click the "Settings" tab.
Click on "Add Translation" and add a new translation.



adp

Monitored Device Details

Host: 192.168.0.63 SOMA Port: 5550 Log Target Source: 192.168.0.63

Device Resources Monitoring: On Service Resources Monitoring: On

Services Operations Portal Settings

Temporary Domain for WSDL Validation and Promotion

Device: Device

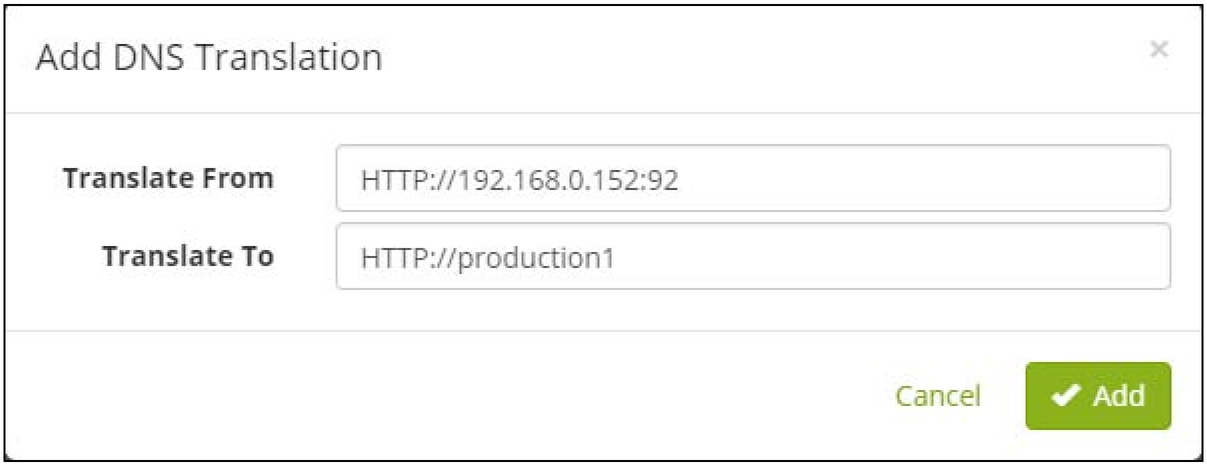
Domain: Domain

The remote and local WSDL validation and promotion operations need to create a temporary DataPower service. Choose a domain where this service will be created. You may use the same domain for multiple devices.

Note: The temporary device needs to be accessible to the device.

DNS Translations for Device

No data to display



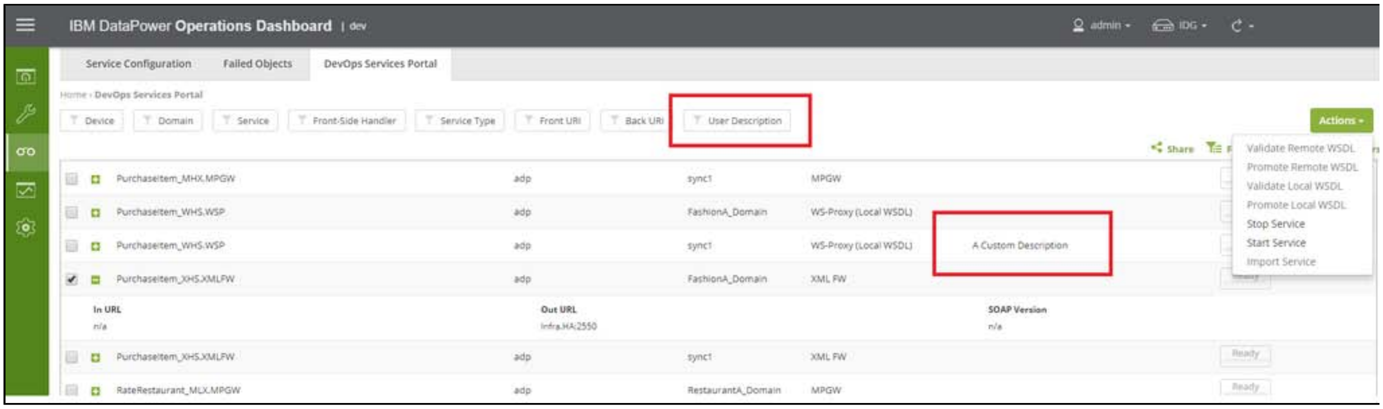
Add DNS Translation

Translate From: HTTP://192.168.0.152:92

Translate To: HTTP://production1

Showing Service User Description in the Services List

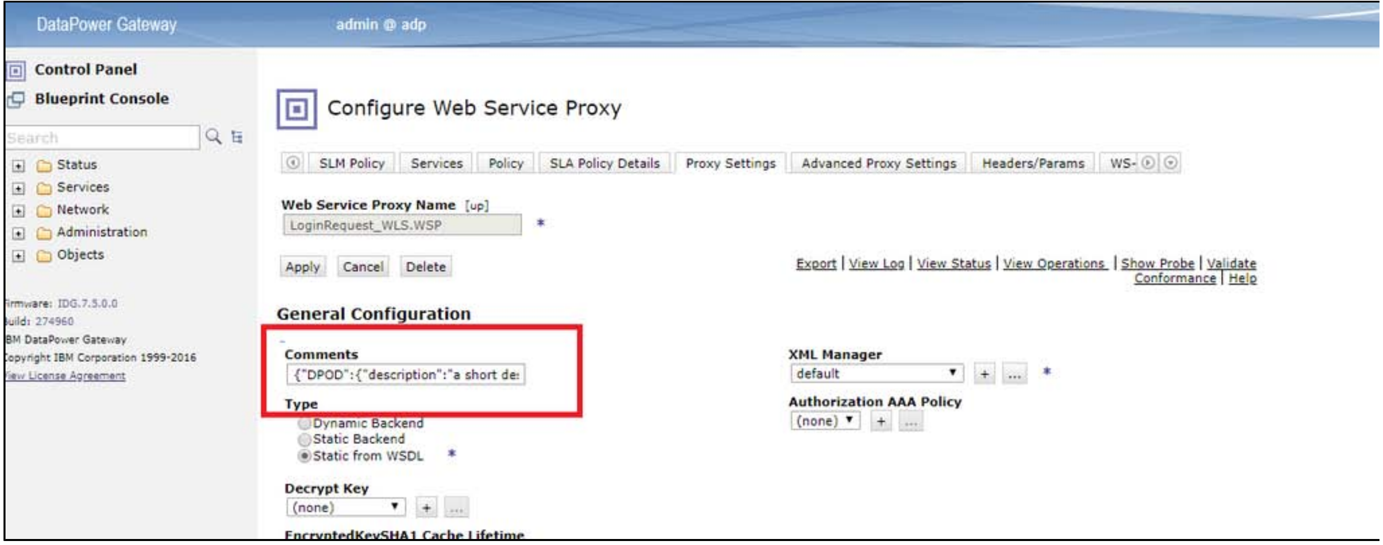
The DevOps Services Portal services list can show a custom user description for each service, users can filter and search by this description.



PurchaseItem_MHX.MPGW	adp	sync1	MPGW	
PurchaseItem_WHS.WSP	adp	FashionA_Domain	WS-Proxy (Local WSDL)	
PurchaseItem_WHS.WSP	adp	sync1	WS-Proxy (Local WSDL)	A Custom Description
PurchaseItem_XHS.XMLFW	adp	FashionA_Domain	XML FW	
PurchaseItem_XHS.XMLFW	adp	sync1	XML FW	
RateRestaurant_MLX.MPGW	adp	RestaurantA_Domain	MPGW	

In URL	Out URL	SOAP Version
n/a	Infra.HA:2550	n/a

DPOD populates the description from the DataPower's comment field of each service.



irmware: IDG.7.5.0.0
uild: 274960
BM DataPower Gateway
opyright IBM Corporation 1999-2016
iew License Agreement

Web Service Proxy Name [up]: LoginRequest_WLS.WSP *

Comments: {"DPOD":{"description":"a short de:

Type: ○ Dynamic Backend ○ Static Backend ● Static from WSDL *

XML Manager: default *

Authorization AAA Policy: (none)

Decrypt Key: (none)

EncryptedKeySHA1 Cache Lifetime

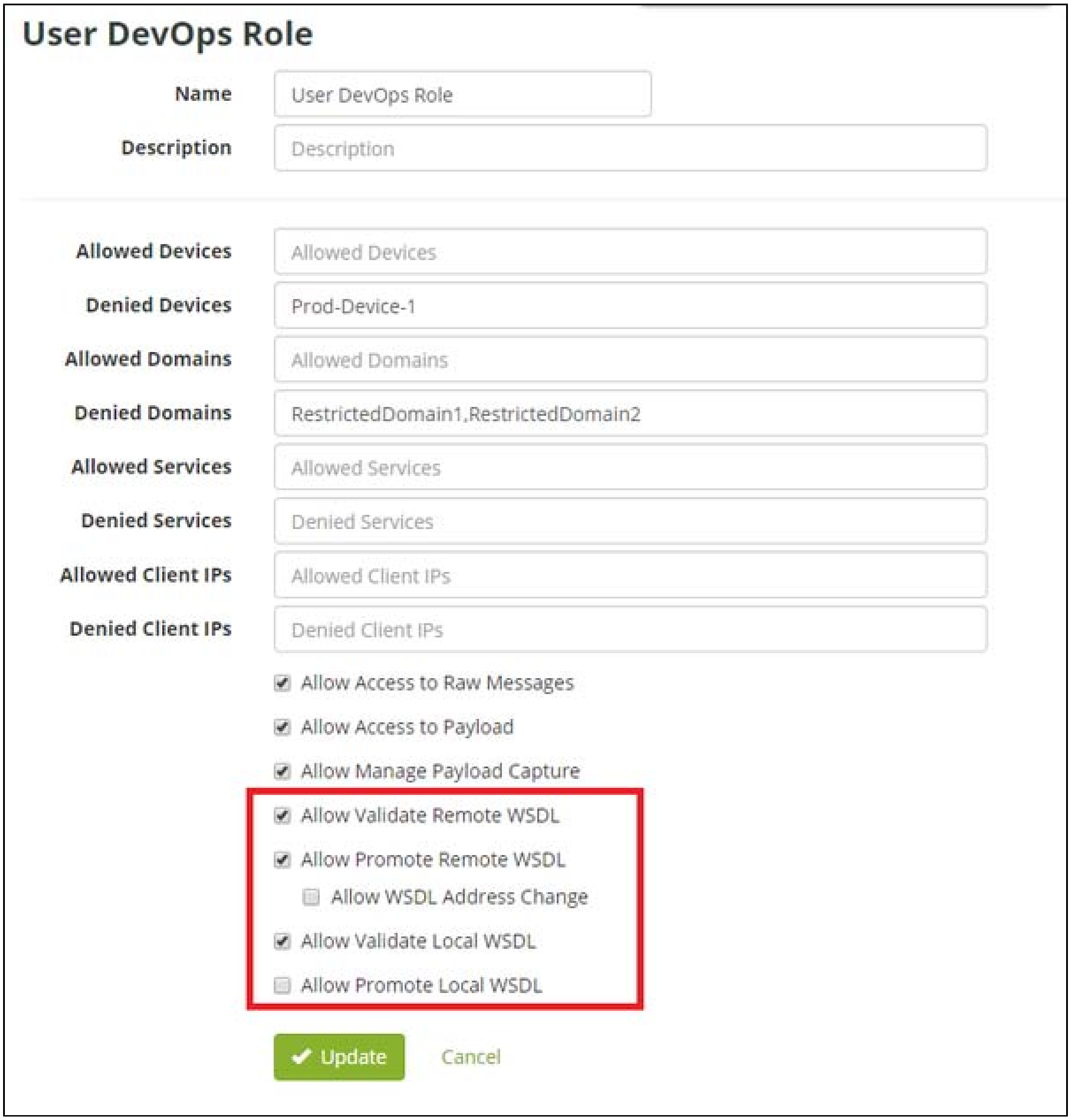
DPOD will populate the value only if it's contained within the following JSON:

Any other formats or comment contents will be ignored

DevOps Portal Security

Access to the DevOps portal page and actions may be controlled in the following ways:

1. Using the Role Based Access Control - add a custom role to the user,
   a. Devices, domains and services will show in the DevOps Portal services list according to the the user's Effective Access Rights
   b. Allow or revoke specific DevOps Portal actions, for Remote WSDL you can also control whether a user can enter or change the WSDL address.
   (Admin users can always perform all DevOps actions, even if they have a role that revokes the action.)



User DevOps Role

Name	User DevOps Role
Description	Description
Allowed Devices	Allowed Devices
Denied Devices	Prod-Device-1
Allowed Domains	Allowed Domains
Denied Domains	RestrictedDomain1,RestrictedDomain2
Allowed Services	Allowed Services
Denied Services	Denied Services
Allowed Client IPs	Allowed Client IPs
Denied Client IPs	Denied Client IPs

☑ Allow Access to Raw Messages
☑ Allow Access to Payload
☑ Allow Manage Payload Capture
☑ Allow Validate Remote WSDL
☑ Allow Promote Remote WSDL
□ Allow WSDL Address Change
☑ Allow Validate Local WSDL
□ Allow Promote Local WSDL

2. From DPOD's system parameters set "Enable Services Portal Operations for non-Admin Users" to completely disable all actions for all non-admin users
   All the actions will be disabled, even if the user has a custom role that allows one or more actions.

Appliance Maintenance

This section contains details and procedures relating to the maintenance tasks required for DPOD.

- Maintenance Concepts
- Configurable Parameters and Settings
- Appliance Backup
- Appliance Configuration Synchronization
- Appliance Firmware Upgrade
- Appliance Migration

Maintenance Concepts

MAINTENANCE ACTIVITY

A maintenance activity defines the set of maintenance actions required for a specific goal. An example of such an activity is "Perform Secure Backup on device X".
Additionally, the maintenance activity contains other specific definitions for the action. This may include for instance which certificate should be used for the Secure Backup or which deployment policy should be used for a configuration sync operation.

MAINTENANCE PLAN

A maintenance activity such as backup or sync is defined inside a plan, e.g. a backup plan, a sync plan etc. A plan only contains a single type of activities.
A plan contains common definitions for all activities included within it, such as scheduling definition, email and syslog addresses to report to, etc.
A plan must contain at least one activity in order for it to be enabled.

MAINTENANCE TASK

A maintenance task is the execution of an operation on a device. An example of a maintenance task would be a secure backup activity on devices QA1 and QA2 which executes two backup tasks - one for each device.

MAINTENANCE WINDOW

A maintenance window defines a period of time during which maintenance plans are allowed to **start** run.
The definition of a maintenance window consists of two parameters in 24h format (e.g. 22:00)

- Maintenance window start time
- Maintenance window end time

A maintenance window may be defined separately for each Maintenance Plan. Alternatively, the installation may use a default system value (see maintenance configurable parameters for more information)
Maintenance Plans will not initiate the execution of any new tasks outside the maintenance window.
If, when the Maintenance Window has ended, some of the plan's tasks are still waiting to execute, they will be marked as cancelled and the plan execution will end. Executing tasks will not be interrupted.

ERROR POLICY

The error policy controls what happen when a task fails (during either validation or execution)
When the error policy is "Halt" - all waiting tasks will be cancelled and will not execute. Executing tasks will not be interrupted.
When the error policy is "Ignore" - remaining tasks will continue to execute as normal.

HOW TO EXECUTE MAINTENANCE PLANS

There are three methods to execute a maintenance plan.
Note that regardless of the method used, to execute a plan it must first be enabled.

1. **Scheduled run:** Enter a value in the plan's schedule field. The format is the same as the one used for scheduling a report
2. **Via REST API:** Consult the Backup REST API or Sync REST API pages for more details
3. **Ad-hoc:** By clicking "Execute" on the Plan Details Page

USING PATTERNS FOR DEVICE AND DOMAIN NAMES

Whenever device or domain patterns are allowed within a plan (e.g. when choosing which devices or domains to backup), DPOD accepts an asterisk to designate a pattern, or a comma to list values

Some examples for device selection are listed below:

Pattern	Details	Selection
Prod*	Asterisk at the end of the pattern	All devices starting with "Prod" e.g. • Prod1 • Prod_Alternate • Prod
*1	Asterisk at the beginning of the pattern	All devices ending with "1" e.g. • Device1 • D1 • Device_External_1

Device_QA_*1	Asterisk in the middle of the pattern	All devices starting with "Device_QA_" and ending with "1" e.g. - Device_QA_Number_1 - Device_QA_1 - Device_QA_With_Alternate_IP_1
Device*QA*	Multiple asterisks in pattern	All devices starting with "Device", having "QA" somewhere in the name e.g - Device_QA - Device_for_QA_of_systems - DeviceQA
Device-QA1, Device-QA2, Device-*3	List of values, with or without asterisk in them	All devices exactly matching values in the list. If an asterisk is used - the rules for asterisks apply e.g. - Device-QA1 (exact name match) - Device-QA2 (exact name match) - Device-QA3 (wildcard match)
*	Asterisk only.	All device names configured in DPOD will be matched.

Configurable Parameters and Settings

This page lists system parameters that are of interest in the appliance maintenance context. The parameters can be configured using the system parameters page.

Parameter	Description	Default Value
Enable Backups	Global flag to enable or disable all backups. No backups will run when this flag is set to false	true
Enable Syncs	Global flag to enable or disable all configuration syncs. No syncs will run when this flag is set to false	true
Enable Firmware Upgrades	Global flag to enable or disable all firmware upgrades. No upgrades will run when this flag is set to false	true
Enable Secure Restores	Global flag to enable or disable all secure restores. No restores will run when this flag is set to false As of DPOD v1.0.9, Secure-Restores are only available via the Appliance Migration feature and not as a stand-alone feature, Disabling this option will disable Appliance Migrations from restoring the target gateway	true
Maintenance User Scripts Source Path	Location of the user Plan/Task Pre/Post scripts in the file system	/app/custom/scripts
Maintenance User Scripts Working Path	The user scripts' execution path. This is normally the same as the source path above	/app/custom/scripts
Maintenance Window Start Time (HH:MM)	Global value for the maintenance window start time. This value may be overridden in a specific plan's settings	22:00
Maintenance Window End Time (HH:MM)	Global value for the maintenance window end time. This value may be overridden in a specific plan's settings	06:00
Maintenance Syslog Notifications Destination Hostname	The hostname or IP address where syslog records are sent to	No Default
Maintenance Syslog Notifications Destination Port	The port where syslog records are sent to	60000
Maintenance Error Syslog Severity Field Value	The severity of error operations syslog records (such as "Plan Failed")	error
Maintenance Success Syslog Severity Field Value	The severity of success syslog records (Such as "Plan Finished Successfully")	info
Maintenance - Timeout in Seconds for Quiesce Operations	The timeout (in seconds) sent to the Quiesce operation when a quiesce operation was requested in the activity. DPOD will add 3 minutes to this timeout and check if all domains quiesced within this period.	1800
Maintenance - Timeout in Seconds for Unquiesce Operations	The timeout (in seconds) for DPOD to wait until all domains unquiesce before marking the task as failed DPOD will add 3 minutes to this timeout	1800
Maintenance - Timeout in Seconds for Restart Operations	The timeout (in seconds) for DPOD to wait for a device to restart before marking the task as failed	1800
Backups - Destination Path	Destination path where DPOD saves its backup files. This path must be a new **dedicated** mounted filesystem (mount point). Backups may not be stored on existing mount point created during DPOD's installation. User can use the Linux command "df -h" to make sure the path entered is a mounted mount point	/data/backups/store
Backups - Backup Store Free Space Threshold (Percent)	Before starting any backup, DPOD ensures that the destination path has enough free storage available. When the percentage of free storage is less than this value, the backup will not proceed	10

Backups - DataPower Temp Free Space Threshold (Percent)	For Secure Backup - the backup will be first stored in the DataPower temp filesystem, Before starting a secure backup, DPOD ensures that the temp DataPower filesystem has enough free storage available. When the percentage of free storage is less than this value, the backup will not proceed	10
Maintenance - Max Minutes Before Marking Task as Canceled	The amount of time (in minutes) DPOD waits before marking a hung task as cancelled. This time is relative to the last status change on the task. When DPOD marks such tasks as cancelled, other tasks may start executing on the device. (The task itself will not be interrupted)	60
Syncs - Temp Files Path	Location where DPOD saves temporary exports and files used by the configuration sync tasks	/app/tmp/sync
Firmware Upgrade - Repository Path	Where DPOD should look for the firmware upgrade image files. It is recommended that you set up a mount point and point the parameter to it. Using the following DPOD paths and subfolders of those paths is not supported: /app /data /logs /installs /var	/tmp
Firmware Upgrade - Local Node IP Address	The network address of DPOD that monitored device can access using SSH	No Default
Firmware Upgrade - OS User Name	DPOD OS user name for SCP access	productuser1
Firmware Upgrade - OS User Password	DPOD OS user password for SCP access	*******
Secure Restore - Seconds to Wait After Restart	When using Secure-Restore, how long to wait after detecting that the gateway is up and running, and before starting post-processing tasks (this time is required for the gateway to process its configuration) As of DPOD v1.0.9, Secure-Restores are only available via the Appliance Migration feature and not as a stand-alone feature.	150
The HTTP Address of the UI	The URL prefix for your DPOD UI - for example: https://10.0.0.50 (everything before /op) it will be used in the maintenance result emails	No Default
Backups - Max Minutes before Releasing Locks on Running Tasks	Maximum time to wait for maintenance task to finish before marking it as cancelled Even when marked as cancelled the maintenance operation may still be executing on the Gateway.	60

Appliance Backup

This section contains information about backing up your DataPower appliance.

- Backup Limitations and Notes
- Backup Plan
- Backup Activity
- Backup Execution (Tasks)
- Backup - User Defined Scripts
- Publish Backup Events via Syslog and Email

Backup Limitations and Notes

This page lists some notes and limitations of the backup process:

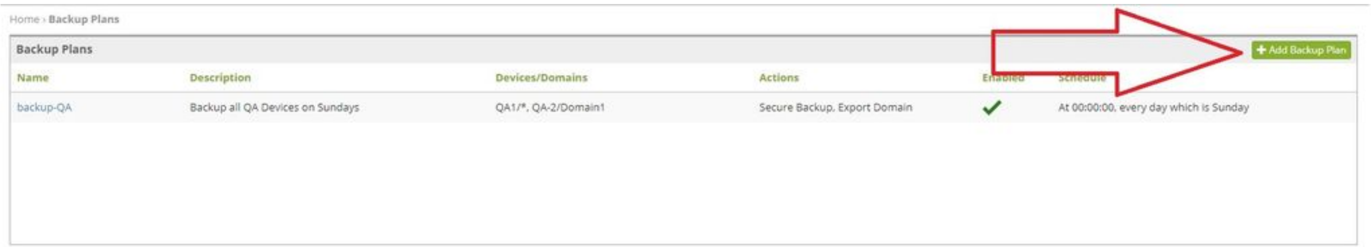
1. The user should define a mounted remote filesystem as the backup destination, see Configurable Parameters and Settings
2. HSM, iSCSI or RAID data is not backed-up
3. API Connect domains are not backed-up, except when in full device backup
4. Only persisted data is backed-up. Unsaved configuration changes will not be backed-up
5. Key materials are only backed up by Secure Backup
6. Administrative operations should not be performed during the backup execution. Doing so may cause failure or inconsistent results
7. Backup of IDG Docker containers is not supported (it may or may not work)

> The backup can only be verified by restoring it to another device and validating its functionality

Backup Plan

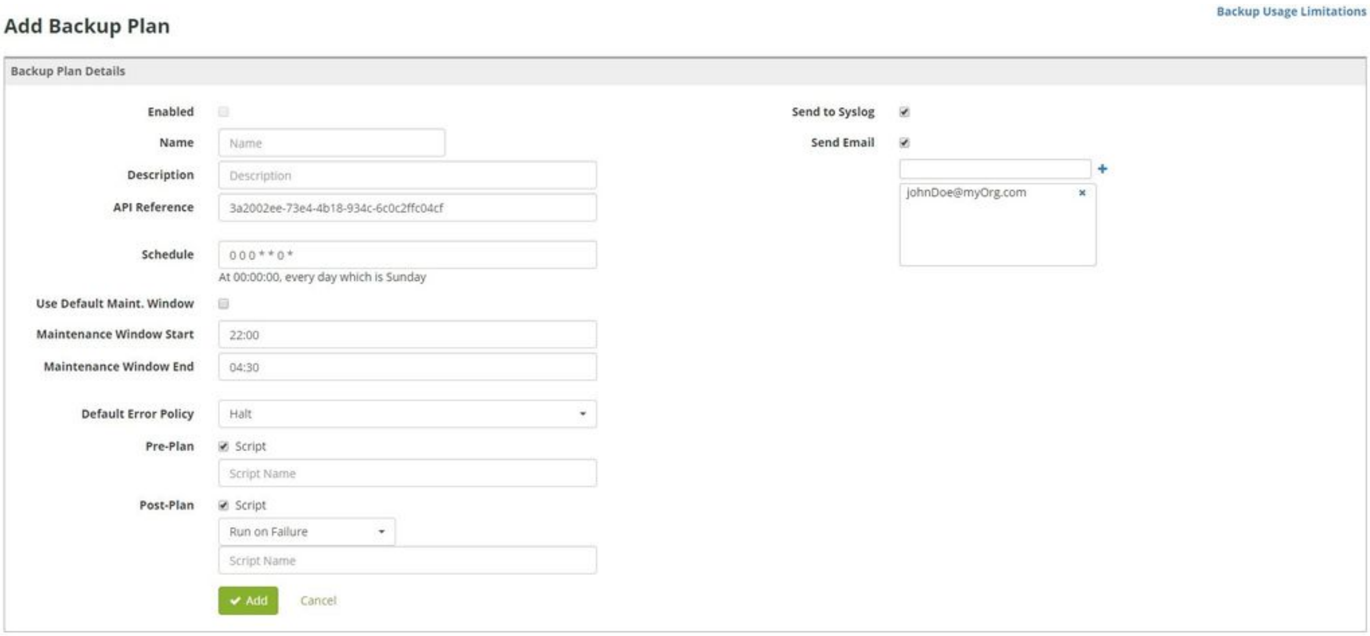
A Backup Plan includes general parameters and definitions for the execution of the backup activities.

To create a new backup plan, navigate to the Manage MaintenanceBackup menu and click on the button to add a new backup plan.



Name	Description	Devices/Domains	Actions	Enabled	Schedule
backup-QA	Backup all QA Devices on Sundays	QA1/*, QA-2/Domain1	Secure Backup, Export Domain	✓	At 00:00:00, every day which is Sunday

The system will display the "Add Backup Plan" page. Consult the screenshot and the table below in order to create a new backup plan in the system.



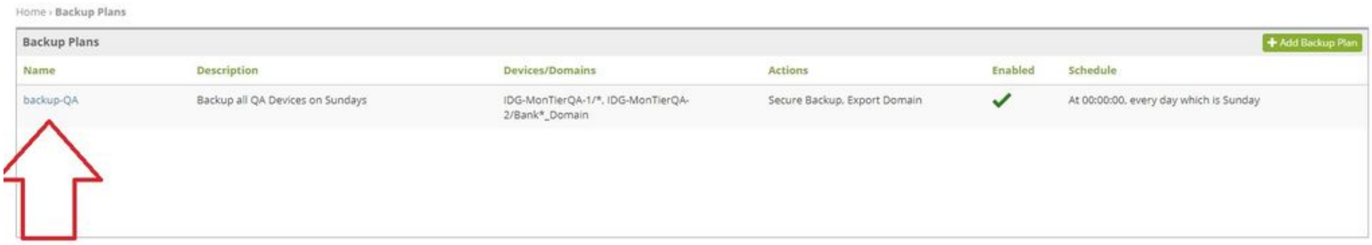
Enabled	□
Name	Name
Description	Description
API Reference	3a2002ee-73e4-4b18-934c-6c0c2ffc04cf
Schedule	0 0 0 * * 0 * At 00:00:00, every day which is Sunday
Use Default Maint. Window	□
Maintenance Window Start	22:00
Maintenance Window End	04:30
Default Error Policy	Halt
Pre-Plan	☑ Script Script Name
Post-Plan	☑ Script Run on Failure Script Name
Send to Syslog	☑
Send Email	☑ johnDoe@myOrg.com

Attribute	Mandatory?	Description
Enabled	Yes	Only enabled plans may be executed, a plan cannot be enabled if it does not contain any activities
Name	Yes	A user-friendly name for the plan, e.g. "BackupQA"
Description	No	A user-friendly description for the plan, e.g. "Backup all QA devices"
API Reference	Yes	A reference that will be used to execute the plan via the Backup REST API. This field is pre-populated with a unique value generated by DPOD, you may change this value.
Schedule	Yes (only for enabled plans)	When to schedule the backup. This field has no effect when the plan is not enabled. Format is identical to the report scheduling format
Use Default Maint. Window	Yes	Should this plan use the default maintenance window defined for the system parameters. (See maintenance configurable parameters for more information)
Maintenance Window Start	No	When not using the system default maintenance window, this will be used as the plan's maintenance window start time in 24H, HH:MM format (e.g. 21:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)
Maintenance Window End	No	When not using the system default maintenance window, this will be used as the plan's maintenance window end time in 24H, HH:MM format (e.g. 06:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)

Default Error Policy	Yes	**Halt** - when a task failed validations or execution, stop all other tasks waiting for execution from this plan. **Ignore** - when a task failed validation or execution, ignore and continue to run other tasks from this plan.
Pre-Plan Script	No	A user defined script to run before any of the tasks is executed. The script will not run if the plan failed validation, e.g. when it is executed outside the maintenance window timeframe. If the script fails (the return code was greater than 0) - the plan will fail too and its tasks will not be executed. See user defined scripts for more information
Post-Plan Script	No	A user defined script to run after all the tasks finished executing. The screen lets the user select whether to always execute this script or execute only when at least one task failed. See user defined scripts for more information
Send to Syslog	No	Send syslog messages for events generated by this plan- see publish backup events via syslogs and email
Send Email	No	Send emails for events generated by this plan - see publish backup events via syslogs and email

The Plan Details Page

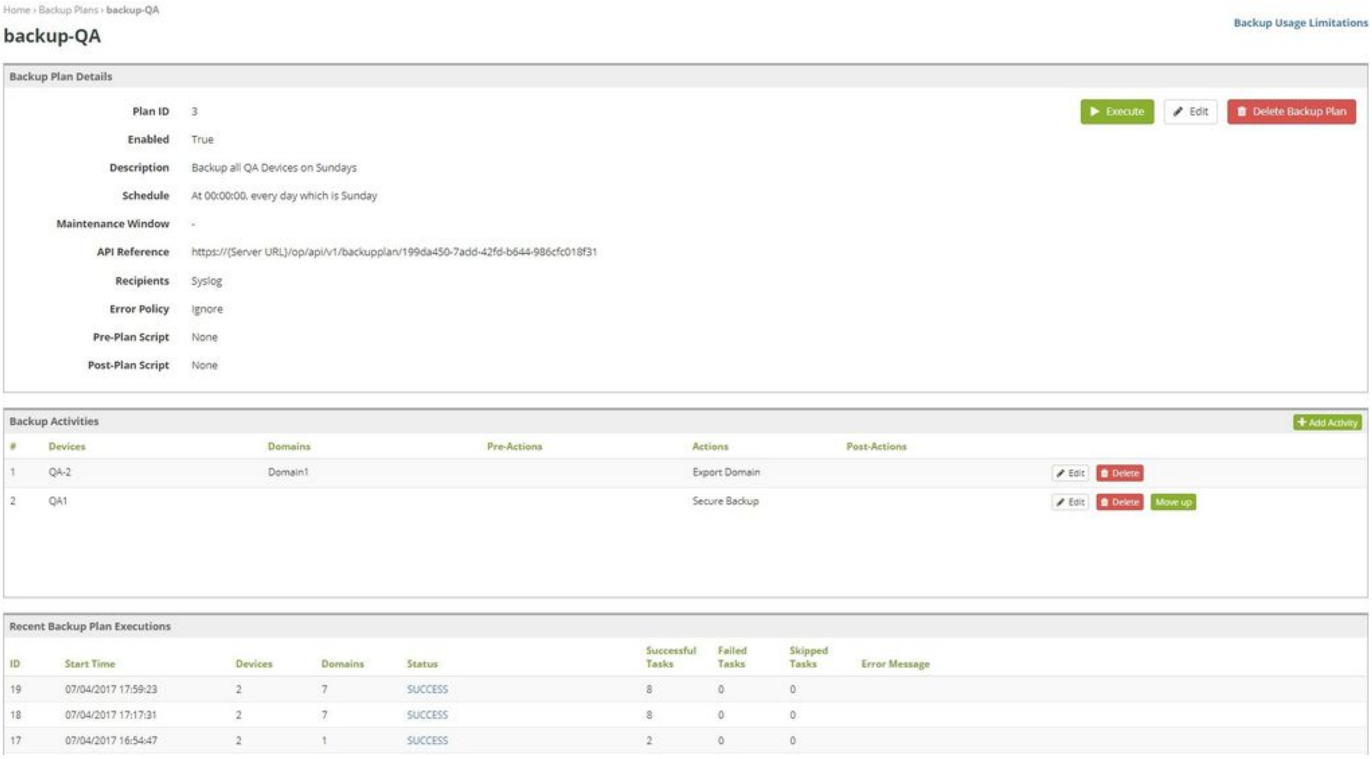
Click the plan's name on the Backup Plans page to display the Plan's Details Page



Name	Description	Devices/Domains	Actions	Enabled	Schedule
backup-QA	Backup all QA Devices on Sundays	IDG-MonTierQA-1/*, IDG-MonTierQA-2/Bank*_Domain	Secure Backup, Export Domain	✓	At 00:00:00, every day which is Sunday

The Plan Details page is composed of three parts:

1. Plan Details - Displays the plan details, and lets the user Edit the plan, Delete it, or execute it in an ad-hoc manner (only for enabled plans)
2. Backup Activities - Add, Edit or Delete a backup activity
3. Recent Backup Plan Executions - Displays results for the most recent 40 executions of the plan - see Maintenance Plans Status Description for descriptions of the possible plan statuses



backup-QA

Backup Plan Details

Plan ID	3
Enabled	True
Description	Backup all QA Devices on Sundays
Schedule	At 00:00:00, every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/backupplan/199da450-7add-42fd-b644-986cfc018f31
Recipients	Syslog
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

Backup Activities

#	Devices	Domains	Pre-Actions	Actions	Post-Actions
1	QA-2	Domain1		Export Domain	
2	QA1			Secure Backup	

Recent Backup Plan Executions

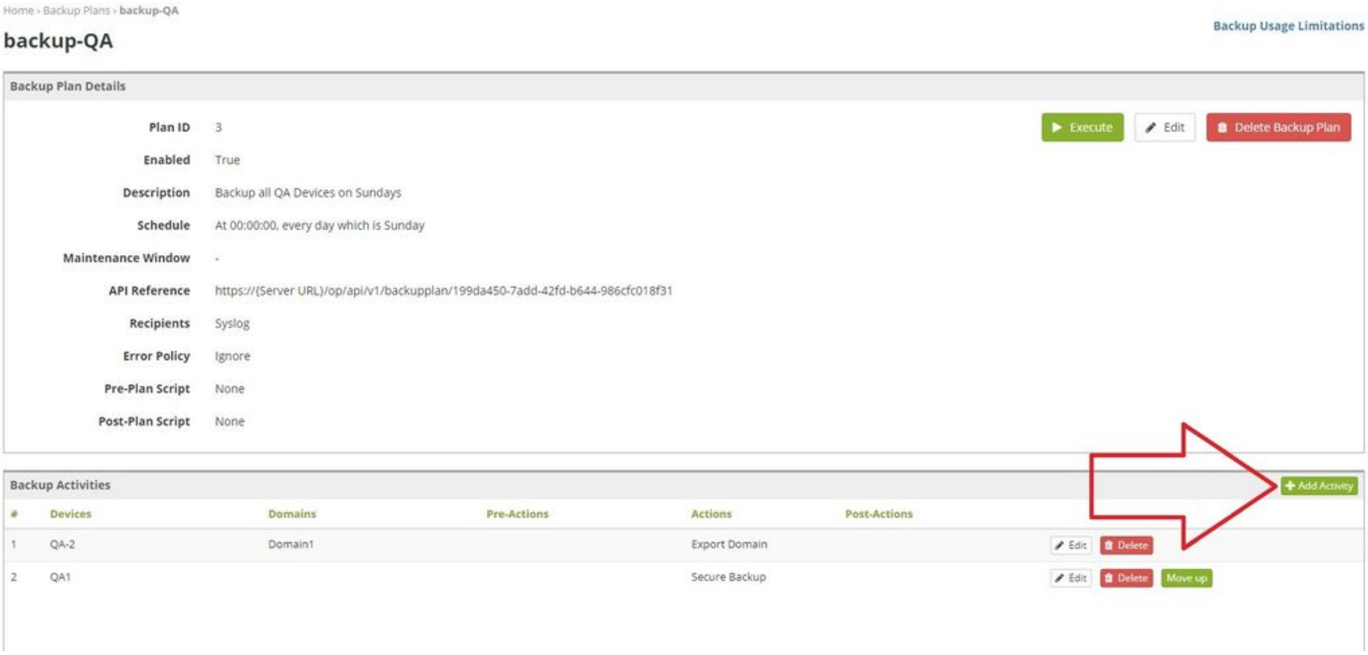
ID	Start Time	Devices	Domains	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
19	07/04/2017 17:59:23	2	7	SUCCESS	8	0	0	
18	07/04/2017 17:17:31	2	7	SUCCESS	8	0	0	
17	07/04/2017 16:54:47	2	1	SUCCESS	2	0	0	

Backup Activity

A Backup Activity defines what should be backed-up, pre/post actions and the error policy to use.
There are two types of activities:

1. Secure Backup
2. Export domain

To add a new backup activity, navigate to Mange Maintenance Backup, select the plan to add an activity to and click "Add Activity" from the Backup Plan Details Page.



backup-QA

Backup Plan Details

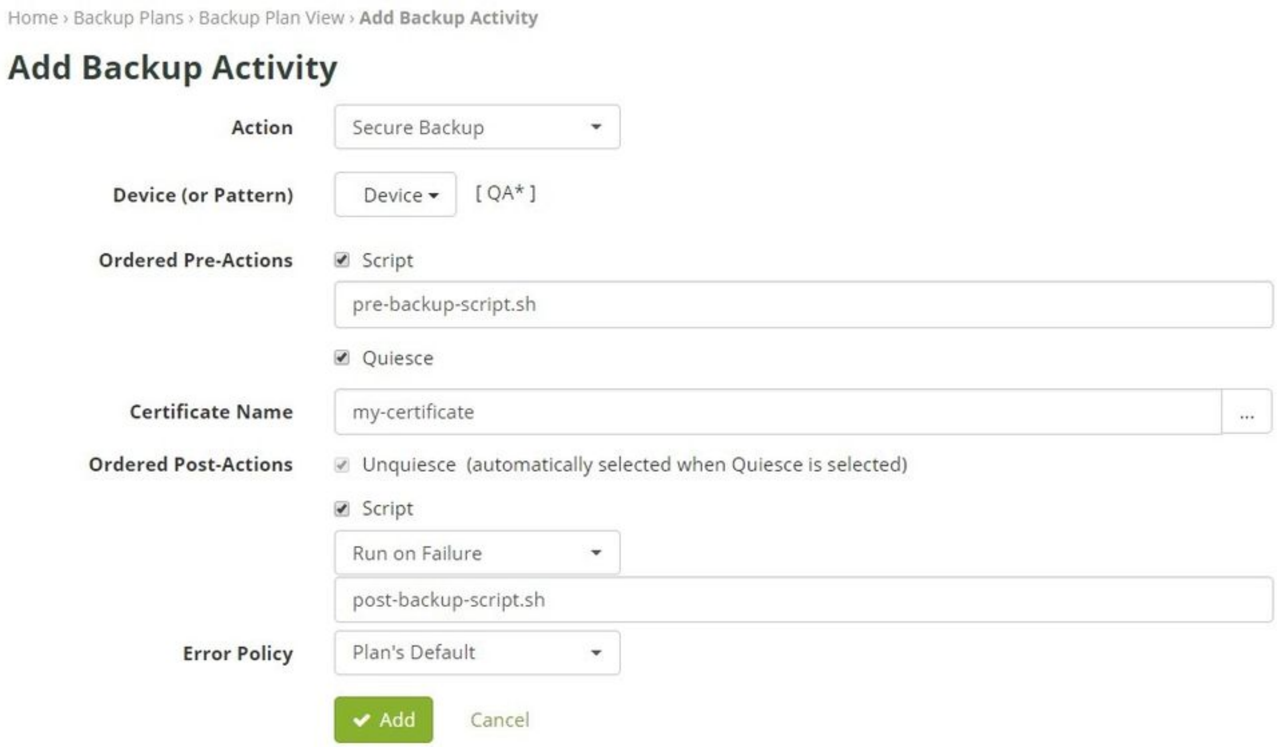
Plan ID	3
Enabled	True
Description	Backup all QA Devices on Sundays
Schedule	At 00:00:00, every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/backupplan/199da450-7add-42fd-b644-986cfc018f31
Recipients	Syslog
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

Backup Activities

#	Devices	Domains	Pre-Actions	Actions	Post-Actions	
1	QA-2	Domain1		Export Domain		Edit Delete
2	QA1			Secure Backup		Edit Delete Move up

The system will display "Add Backup Activity" page. Consult the screenshot and the table below in order to create a new backup activity in the system.

Secure Backup



Home › Backup Plans › Backup Plan View › **Add Backup Activity**

Add Backup Activity

Action: Secure Backup

Device (or Pattern): Device [QA*]

Ordered Pre-Actions: ☑ Script

pre-backup-script.sh

☑ Quiesce

Certificate Name: my-certificate ...

Ordered Post-Actions: ☑ Unquiesce (automatically selected when Quiesce is selected)

☑ Script

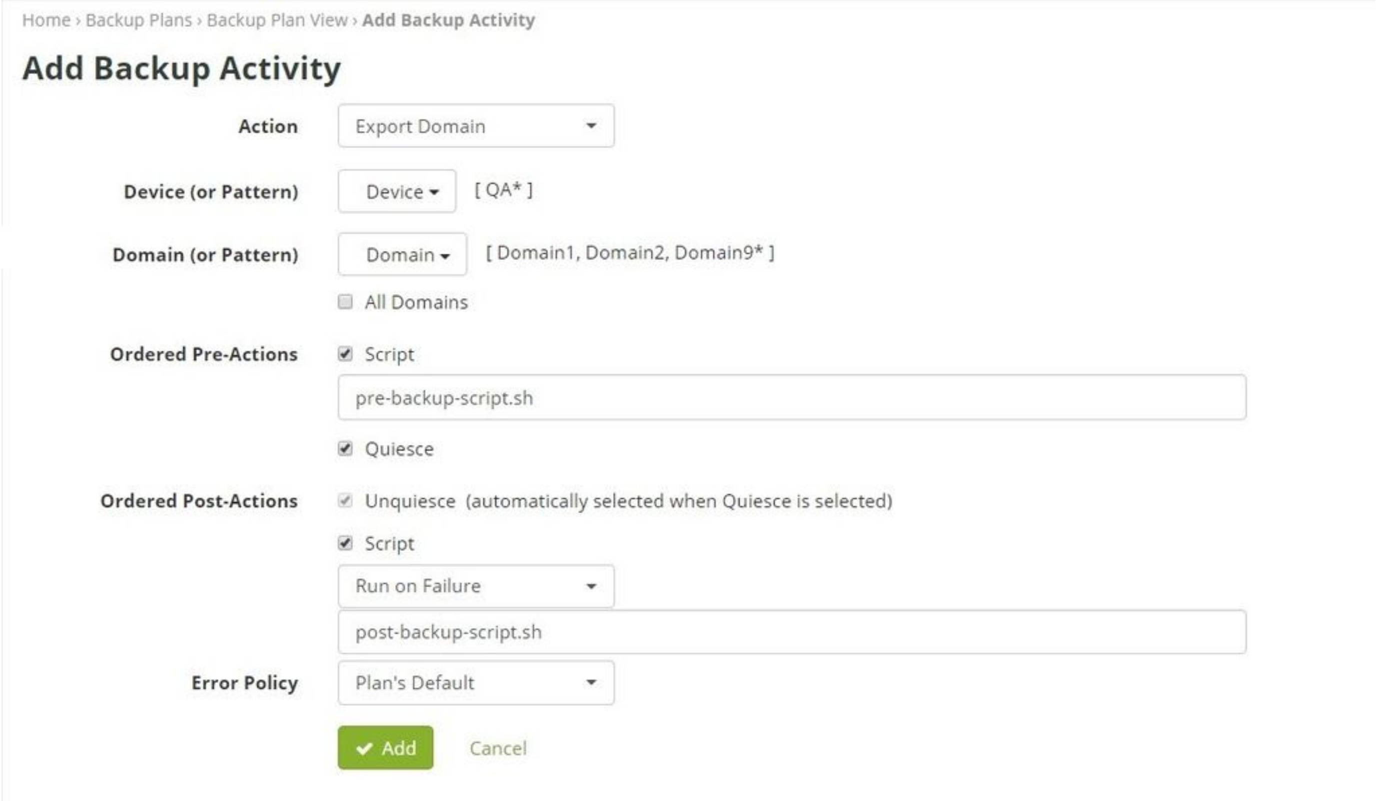
Run on Failure

post-backup-script.sh

Error Policy: Plan's Default

Attribute	Is Mandatory?	Description
Device (or Pattern)	Yes	The Device(s) to backup, enter a specific device, pattern with asterisk or a list of devices or patterns See Using Patterns for Device and Domain Names in the Maintenance Concepts page
Pre-Action Script	No	A user defined script to run before the task is executed. The task will not be executed If the script fails (the return code was greater than 0) See user defined scripts for more information
Pre-Action Quiesce	No	Should the device(s) be quiesced before the backup is executed. The timeout value that is passed to the quiesce SOMA is controlled by a system parameter (see maintenance configurable parameters for more information)
Action	Yes	Select Secure Backup to define a secure backup activity. (Export Domain is described below)
Certificate Name	Yes	The certificate to use for the backup. Click on the ... (Three dots) button to open a window that shows the available certificates on the device, if multiple devices were chosen, the list will show the certificates of the first device. All other devices must have a certificate installed with an identical name to the one selected for the first device.
Post-Action Unquiesce	No	This option cannot be edited - it will be automatically set to the value of the Pre-Action Quiesce. The user may set how long DPOD waits for the unquiesce operation to finish before cancelling the task via a system parameter (see maintenance configurable parameters for more information)
Post-Action Script	No	A user defined script to run after the task is executed. The user selects whether the script should run always when a task completes, or only when the task execution fails. See user defined scripts for more information
Error Policy	Yes	Select how this backup activity handles errors. **Plan's Default** - Use the value that was set for the plan **Halt** - When the task failed validation or execution, stop all other tasks from this plan that are waiting for execution **Ignore** - When the task failed validation or execution, ignore and continue to run other tasks from this plan

Export Domain



Home › Backup Plans › Backup Plan View › **Add Backup Activity**

Add Backup Activity

Action Export Domain ▾

Device (or Pattern) Device ▾ [QA*]

Domain (or Pattern) Domain ▾ [Domain1, Domain2, Domain9*]

□ All Domains

Ordered Pre-Actions ☑ Script

pre-backup-script.sh

☑ Quiesce

Ordered Post-Actions ☑ Unquiesce (automatically selected when Quiesce is selected)

☑ Script

Run on Failure ▾

post-backup-script.sh

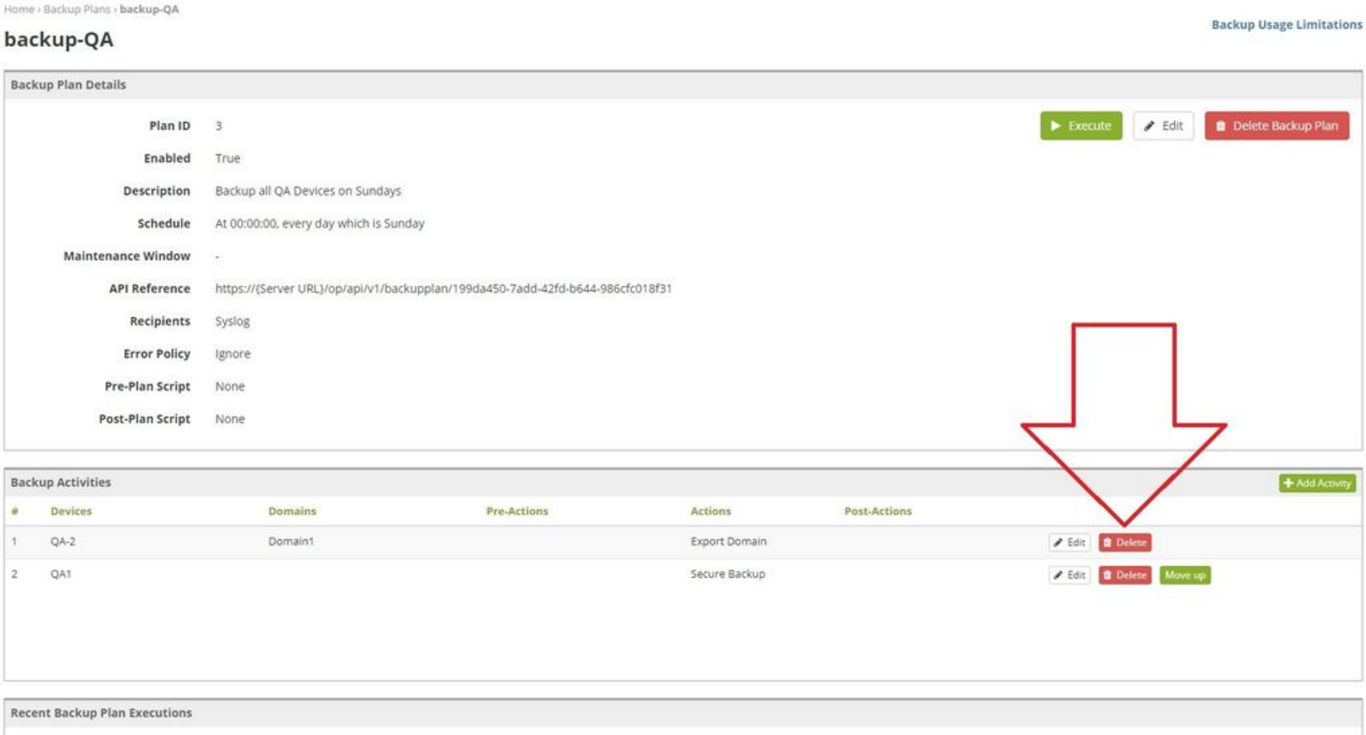
Error Policy Plan's Default ▾

Attribute	Mandatory?	Description
Device (or Pattern)	Yes	The device(s) to backup. Enter a specific device, pattern with asterisk or a list of devices or patterns See Using Patterns for Device and Domain Names in the Maintenance Concepts page
Domain (or Pattern)	Yes	The domain(s) to export. Enter a specific domain, pattern with asterisk or a list of domains or patterns See Using Patterns for Device and Domain Names in the Maintenance Concepts page Check "All Domains" to export all domains.
Pre-Action Script	No	A user defined script to run before the task is executed. The task will not be executed If the script fails (the return code was greater than 0) See user defined scripts for more information
Pre-Action Quiesce	No	Should the domain(s) be quiesced before the backup is executed The timeout value that is passed to the quiesce SOMA is controlled by a system parameter (see maintenance configurable parameters for more information)
Action	Yes	Export Domain
Post-Action Unquiesce	No	This option cannot be edited - it will be automatically set to the value of the Pre-Action Quiesce. The user may set how long DPOD waits for the unquiesce operation to finish before cancelling the task via a system parameter (see maintenance configurable parameters for more information)
Post-Action Script	No	A user defined script to run after the task is executed. The user selects whether the script should run always when a task completes, or only when the task execution fails. See user defined scripts for more information

Error Policy	Yes	Select how this backup activity handles errors. **Plan's Default** - Use the value that was set for the plan **Halt** - When the task failed validation or execution, stop all other tasks from this plan that are waiting for execution **Ignore** - When the task failed validation or execution, ignore and continue to run other tasks from this plan

Edit, Delete or Reorder Activities

The Backup Plan Details Page allows the user to edit, delete or reorder activities.
When the plan is scheduled to run, the activities will be processed in the order they were defined (see Backup Execution for more information)



backup-QA

Backup Plan Details

Plan ID	3
Enabled	True
Description	Backup all QA Devices on Sundays
Schedule	At 00:00:00, every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/backupplan/199da450-7add-42fd-b644-986cfc018f31
Recipients	Syslog
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

Backup Activities

#	Devices	Domains	Pre-Actions	Actions	Post-Actions
1	QA-2	Domain1		Export Domain	
2	QA1			Secure Backup	

Recent Backup Plan Executions

Backup Execution (Tasks)

This page describes how DPOD prepares the execution flow of a backup plan (using tasks) and subsequently - how the tasks themselves are executed.

Task Creation Flow

General execution flow for a backup plan:

1. Verify that the system allows Backups to run. (See Configurable Parameters and Settings to learn how to enable or disable all backup activities)
2. Verify that the current system time is within the maintenance window timeframe defined for the plan
3. Verify that the backup store destination path is a mounted, remote, filesystem. (See Configurable Parameters and Settings to learn how to set the destination path)
4. Verify that there is enough space in the destination path for downloading and storing the backup. (See Configurable Parameters and Settings to learn how to determine this check's threshold value)
5. Iterate over all the activities defined for the plan, and split them into executable tasks.
   For example: consider a plan with two activities, one to Secure Backup devices QA* and a second to export domain DOMAIN* on device TEST8 and on an unavailable device - TEST9.
   DPOD will create six tasks:
   a. Secure Backup task for device QA1
   b. Secure Backup task for device QA2
   c. Secure Backup task for device QA3
   d. Export Domain task for Device TEST8 and Domain DOMAIN1
   e. Export Domain task for Device TEST8 and Domain DOMAIN2
   f. Export Domain task for Device TEST9 and domain DOMAIN*. Note: this task will be created with a "Skipped" status since the device TEST9 is unavailable.
6. If all the created tasks are in "Skipped" state (because the devices are not available, or because no devices or domains matched the input patterns) - the plan will stop
7. If there are any tasks waiting to be executed - the Pre-Plan Script will be executed (if requested in the plan settings)
   .the plan will stop if the script's return code is larger than 0

Task Execution Flow

After the backup tasks are created, they will start to execute. The following is the general execution flow for a backup task:

> Backup tasks will start to execute in the order they were created, which corresponds to the order which the activities were defined.
> Two different tasks will not execute concurrent backups on the same device, even if they backup different domains.

1. Verify that the current system time is within the maintenance window timeframe defined for the plan.
2. Verify that there is enough space in the destination path for downloading and storing the files. (See Configurable Parameters and Settings to lean how to determine the check threshold value)
3. If the backup is for a specific domain and quiesce was requested - check that the domain is not already quiesced
   If the backup is for an entire device and quiesce was requested - check that there are no quiesced domains on the device
4. If Export Domain was requested - check that there are no unsaved changes in the requested domain(s),
   If there are any unsaved changes, two export domain backups will be taken - one for the persisted data and one for the unpersisted data.
5. If Secure Backup was requested - check that there is enough space in the DataPower appliance to store the backup before downloading it to the user storage. (See Configurable Parameters and Settings to learn how to determine this check's threshold value)
6. Run the user's pre-script (if requested in the activity), the task will stop if the script return value is larger than 0
7. Issue a Quiesce domain/device SOMA (if requested for the activity)
8. Wait for the device or domain to finish quiescing. A timeout value may be specified for the Quiesce SOMA (see Configurable Parameters and Settings),
   DPOD will cancel the task if the domain(s) are not yet quiesced 3 minutes after the specified timeout, and will issue an Unquiesce SOMA
9. Perform the Secure Backup or Export Domain operation
10. Unquiesce the device/domain (if it was previously quiesced by this task)
11. Wait for the device/domain to unquiesce. A timeout value may be specified for this operation. 3 minutes after the timeout, DPOD will stop waiting for the unquiesce operation and will fail the task (the device's unquiesce operation will not be interrupted though)
12. Run the user's post-task script (if requested in the activity)

When all the plan's tasks completed execution, the post-plan script will be executed (if requested in the plan settings)

Output Files

The backups will be downloaded and stored in the destination filesystem that was set by the user (see Configurable Parameters and Settings)

For **secure backup,** the destination path will be:
<user defined path> + /Device-Name/secure-backup/timestamp
E.g. /data/backup/store/QA-device1/secure-backup/2017-06-26-22-48-00-000

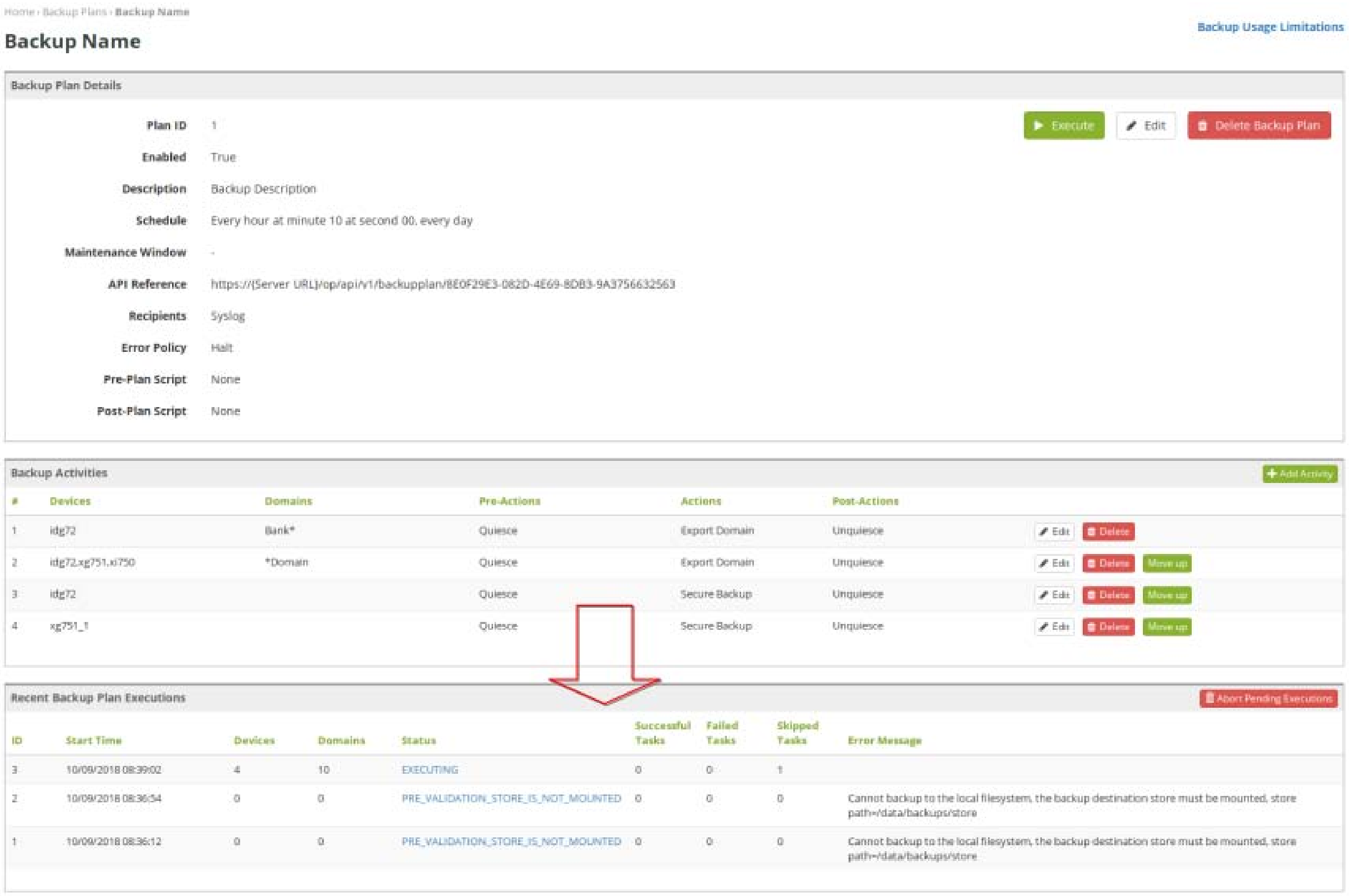
For **export domain (specific domain)**, the destination path will be:

<user defined path> + /Device-Name/domain/domain-name/domain-export-timestamp-isPersisted
E.g. /data/backup/store/QA-device1/domain/Domain1/Domain1-export-2017-06-26-22-48-00-000-persisted.zip

For **export domain (all domains)**, the destination path will be:
<user defined path> + /Device-Name/domain/all-domains/all-domains-export-timestamp-isPersisted
E.g. /data/backup/store/QA-device1/all-domains/all-domains-export-2017-06-26-22-48-00-000-nonpersisted.zip

Backup Execution Results

The Plan Details page shows the 40 most recent plan execution results,



Backup Name

Backup Plan Details

Plan ID	1
Enabled	True
Description	Backup Description
Schedule	Every hour at minute 10 at second 00, every day
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/backupplan/8E0F29E3-082D-4E69-8DB3-9A3756632563
Recipients	Syslog
Error Policy	Halt
Pre-Plan Script	None
Post-Plan Script	None

Backup Activities

#	Devices	Domains	Pre-Actions	Actions	Post-Actions
1	idg72	Bank*	Quiesce	Export Domain	Unquiesce
2	idg72,xg751,xi750	*Domain	Quiesce	Export Domain	Unquiesce
3	idg72		Quiesce	Secure Backup	Unquiesce
4	xg751_1		Quiesce	Secure Backup	Unquiesce

Recent Backup Plan Executions

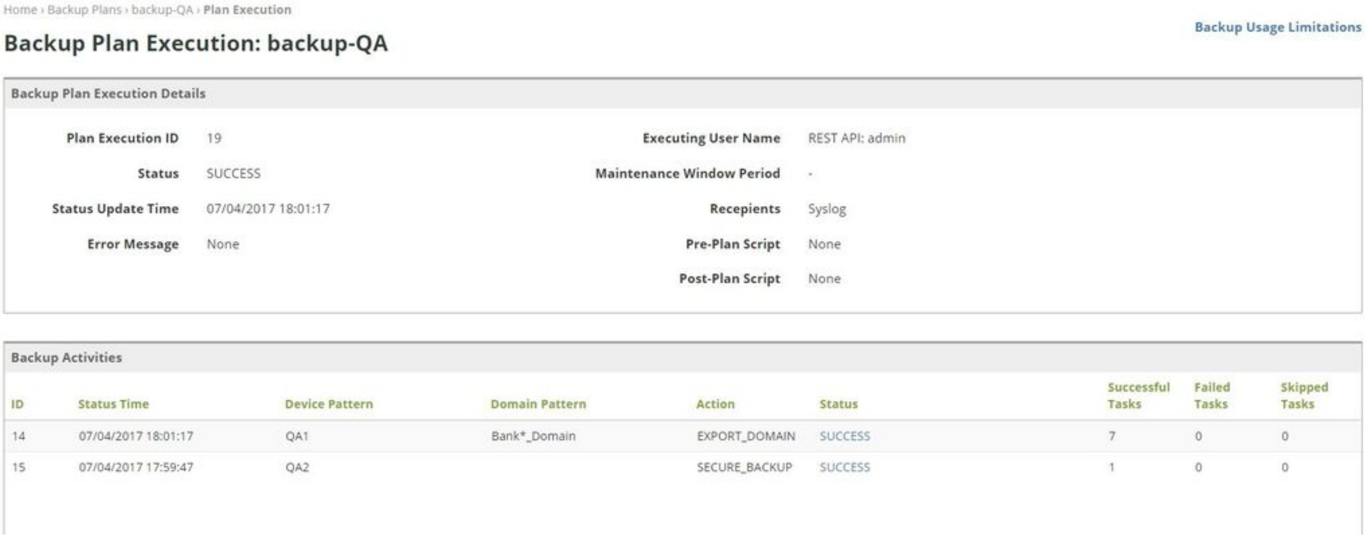
ID	Start Time	Devices	Domains	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
3	10/09/2018 08:39:02	4	10	EXECUTING	0	0	1	
2	10/09/2018 08:36:54	0	0	PRE_VALIDATION_STORE_IS_NOT_MOUNTED	0	0	0	Cannot backup to the local filesystem, the backup destination store must be mounted, store path=/data/backups/store
1	10/09/2018 08:36:12	0	0	PRE_VALIDATION_STORE_IS_NOT_MOUNTED	0	0	0	Cannot backup to the local filesystem, the backup destination store must be mounted, store path=/data/backups/store

The table outlines the following details for each plan execution

Column Name	Description
ID	The Plan Execution ID
Start Time	The time the plan entered the execution queue
Devices	Number of devices that were supposed to be backed-up. Both failed and successful backups are aggregated.
Domains	Number of domains that were supposed to be backed-up. Both failed and successful backups are aggregated. (Note: no domains are aggregated for secure backup and export all domains)
Status	The current status of the plan
Successful Tasks	Number of backup tasks that completed successfully for this plan execution
Failed Tasks	Number of backup tasks that failed for this plan execution

Skipped Tasks	Number of backup tasks that did not execute, e.g. because the device was not available
Error Message	Plan's Error message (If any)

*Click the red "Abort Pending Executions" to stop execution in status "WAITING_FOR_PRE_VALIDATION" that did not started yet.
**Click the status column to drill into the activities execution details page.



Home › Backup Plans › backup-QA › Plan Execution

Backup Plan Execution: backup-QA

Backup Usage Limitations

Backup Plan Execution Details

Plan Execution ID 19

Status SUCCESS

Status Update Time 07/04/2017 18:01:17

Error Message None

Executing User Name REST API: admin

Maintenance Window Period -

Recepients Syslog

Pre-Plan Script None

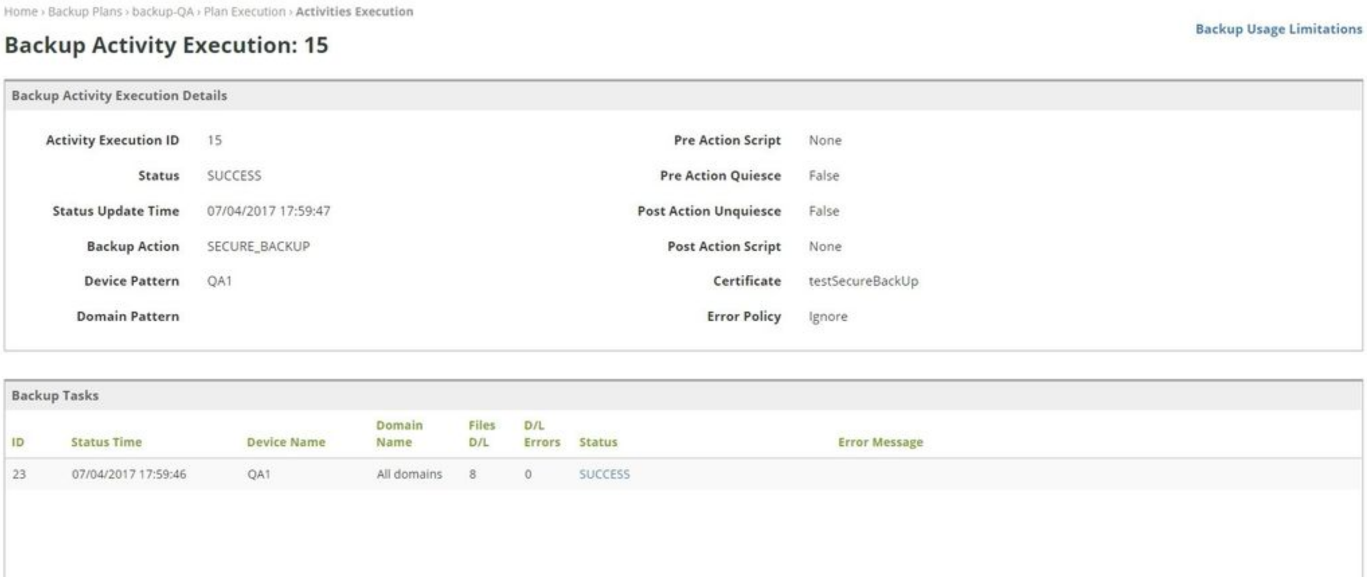
Post-Plan Script None

Backup Activities

ID	Status Time	Device Pattern	Domain Pattern	Action	Status	Successful Tasks	Failed Tasks	Skipped Tasks
14	07/04/2017 18:01:17	QA1	Bank*_Domain	EXPORT_DOMAIN	SUCCESS	7	0	0
15	07/04/2017 17:59:47	QA2		SECURE_BACKUP	SUCCESS	1	0	0

Column Name	Description
ID	The Activity Execution ID
Status Time	The last time the status of the activity changed
Device Pattern	The device name or pattern that was used for this backup activity
Domain Pattern	The domain name or pattern that was used for this backup activity
Action	SECURE_BACKUP or EXPORT_DOMAIN
Status	The current status of the activity
Successful Tasks	Number of backup tasks that completed successfully for this activity execution
Failed Tasks	Number of backup tasks that failed for this activity execution
Skipped Tasks	Number of backup tasks that were skipped for this activity execution

Click the status column to drill into the task execution details page



Home › Backup Plans › backup-QA › Plan Execution › **Activities Execution**

Backup Usage Limitations

Backup Activity Execution: 15

Backup Activity Execution Details

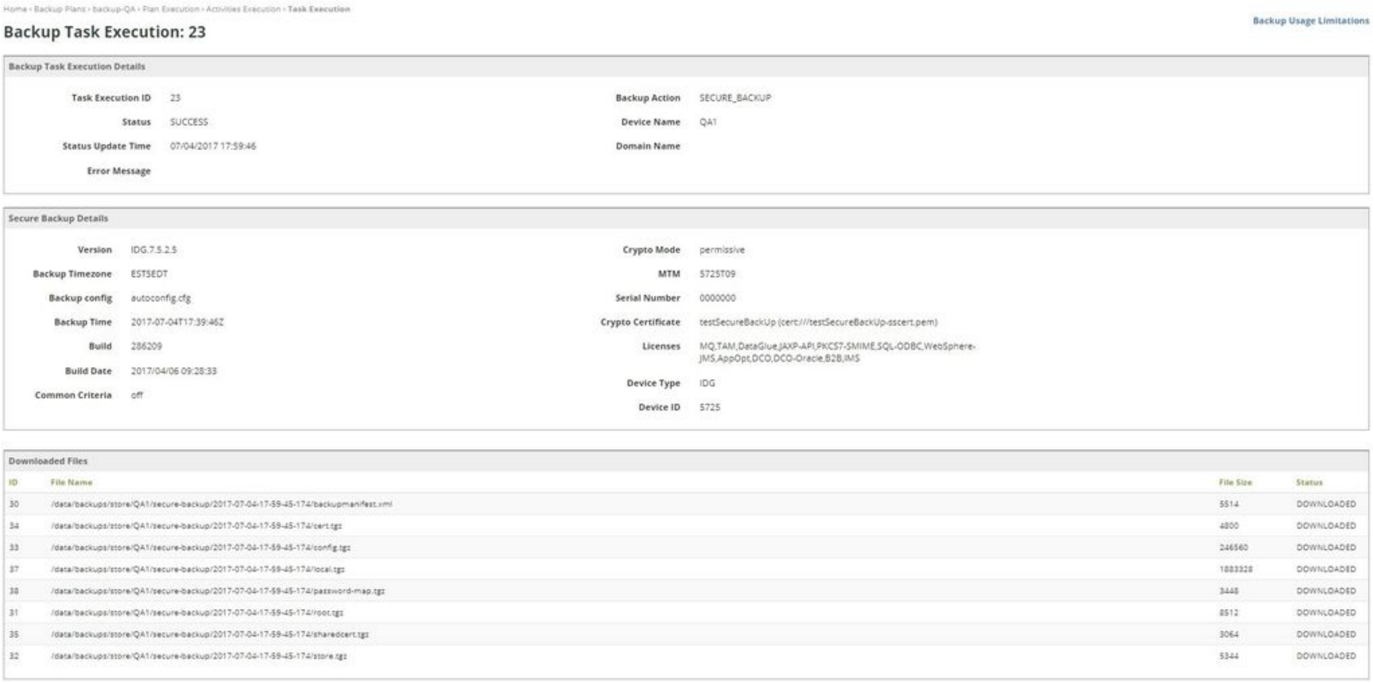
Activity Execution ID	15	**Pre Action Script**	None
Status	SUCCESS	**Pre Action Quiesce**	False
Status Update Time	07/04/2017 17:59:47	**Post Action Unquiesce**	False
Backup Action	SECURE_BACKUP	**Post Action Script**	None
Device Pattern	QA1	**Certificate**	testSecureBackUp
Domain Pattern		**Error Policy**	Ignore

Backup Tasks

ID	Status Time	Device Name	Domain Name	Files D/L	D/L Errors	Status	Error Message
23	07/04/2017 17:59:46	QA1	All domains	8	0	SUCCESS	

Column Name	Description
ID	The Task Execution ID
Status Time	The last time the status of the task changed
Device Name	The Device being backed-up
Domain Name	The Domain being backed-up or "all-domains" for Secure Backup/Export Domain for all domains
Files D/L	Number of files that were downloaded to the user's storage
D/L Errors	Number of download errors
Status	The current status of the task
Error Message	Task's Error message if any

Click the status column to drill into the downloaded files details page



Home › Backup Plans › backup-QA › Plan Execution › Activities Execution › **Task Execution**

Backup Usage Limitations

Backup Task Execution: 23

Backup Task Execution Details

Task Execution ID	23	**Backup Action**	SECURE_BACKUP
Status	SUCCESS	**Device Name**	QA1
Status Update Time	07/04/2017 17:59:46	**Domain Name**	
Error Message			

Secure Backup Details

Version	IDG.7.5.2.5	**Crypto Mode**	permissive
Backup Timezone	EST5EDT	**MTM**	5725T09
Backup config	autoconfig.cfg	**Serial Number**	0000000
Backup Time	2017-07-04T17:39:46Z	**Crypto Certificate**	testSecureBackUp (cert:///testSecureBackUp-sscert.pem)
Build	286209	**Licenses**	MQ,TAM,DataGlue,JAXP-API,PKCS7-SMIME,SQL-ODBC,WebSphere-JMS,AppOpt,DCO,DCO-Oracle,B2B,IMS
Build Date	2017/04/06 09:28:33	**Device Type**	IDG
Common Criteria	off	**Device ID**	5725

Downloaded Files

ID	File Name	File Size	Status
30	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/backupmanifest.xml	5514	DOWNLOADED
34	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/cert.tgz	4800	DOWNLOADED
33	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/config.tgz	246560	DOWNLOADED
37	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/local.tgz	1883328	DOWNLOADED
38	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/password-map.tgz	3448	DOWNLOADED
31	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/root.tgz	8512	DOWNLOADED
35	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/sharedcert.tgz	3064	DOWNLOADED
32	/data/backups/store/QA1/secure-backup/2017-07-04-17-59-45-174/store.tgz	5344	DOWNLOADED

The downloaded files page displays information about the backup operation, such as the device firmware version, device type, device build, etc; and a list of all files that were downloaded to the user's storage

Backup - User Defined Scripts

DPOD allows execution of user defined, custom scripts before and after both Plan and Task execution.
The scripts are executed from /app/custom/scripts (See Configurable Parameters and Settings for information on how to change this path)

> Any script that returns a return code larger than 0 is considered to have failed.
>
> if a pre-plan or a pre-task script failed - the plan or task will be flagged as failed and will **not** execute.
> If a pre-task script failed, the post-task script will still be executed (if requested)

DPOD will send certain parameters to the script, to indicate the execution details and completion status.

Parameters Sent to the Backup Pre-Plan Script

Sample script: /app/custom/scripts/backup_pre_plan_sample.sh

1=PLAN_TYPE - The constant "BACKUP-PLAN"
2=PLAN_STAGE - The constant "PRE"
3=PLAN_ID - The ID of the backup plan
3=PLAN_NAME - The name of the backup plan

Example:
1=BACKUP-PLAN
2=PRE
3=16
4=backup1

Parameters Sent to the Backup Post-Plan Script

Sample script: /app/custom/scripts/backup_post_plan_sample.sh

1=PLAN_TYPE - The constant "BACKUP-PLAN"
2=PLAN_STAGE - The constant "POST"
3=PLAN_ID - The ID of the backup plan
4=PLAN_NAME - The name of the backup plan
5=FINAL_STATUS_CODE - Final status code of the backup plan
6=FINAL_ERROR_MSG - Final error message of the backup plan, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=TASKS_VALUES - list of comma separated values for each task - task ID, backup action, device, domain, task status - different tasks are separated with ~ (Tilde sign)

Example:
1=BACKUP-PLAN
2=POST
3=16
4=backup1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=13,exportDomain,IDG-MonTierQA-2,CarRentA_Domain,SUCCESS~14,exportDomain,IDG-QA-2,CarRentB_Domain,SUCCESS

Parameters Sent to the Backup Pre-Task Script

Sample script: /app/custom/scripts/backup_pre_task_sample.sh

1=TASK_TYPE - The constant "BACKUP-TASK"
2=TASK_STAGE - The constant "PRE"
3=TASK_ID - The ID of the backup task
4=PLAN_NAME - The name of the backup plan that generated this task
5=BACKUP_ACTION - The action that the backup task is going to perform: One of "exportDomain" or "secureBackup"
6=DEVICE_NAME - The name of the device that will be backed-up by the task (or contains the domain to be backed-up)
7=DEVICE_HOST - The host of the device that will backed-up by the task (or contains the domain to be backed-up)
8=SOMA_PORT - The soma port of the device
9=DOMAIN - The name of the domain that will be backed-up by the task, or the constant "ALL" in case of secureBackup

Example:
1=BACKUP-TASK
2=PRE

3=12
4=backup1
5=exportDomain
6=IDG-QA-2
7=192.168.72.100
8=5550
9=CarRentalA_Domain

Parameters Sent to the Backup Post-Task Script

Sample script: /app/custom/scripts/backup_post_task_sample.sh

1=TASK_TYPE - The constant "BACKUP-TASK"
2=TASK_STAGE - The constant "POST"
3=TASK_ID - The ID of the backup task
4=PLAN_NAME - The name of the backup plan that generated this task
5=FINAL_STATUS - Final status code of the backup task
6=FINAL_ERROR_MSG - Final error message of the backup task, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=BACKUP_ACTION - The action that the backup task performed. One of "exportDomain" or "secureBackup"
10=DEVICE_NAME - The name of the device that was backed-up by the task (or contains the domain that was backed-up)
11=DEVICE_HOST - The host of the device that was backed-up by the task (or contains the domain that was backed-up)
12=SOMA_PORT - The soma port of the device
13=DOMAIN - The name of the domain that was backed-up by the task, or the constant "ALL" in case of secureBackup
14=DOWNLOADED_FILES - comma separated list of downloaded backup files (full path) or the constant "NONE"

Example:
1=BACKUP-TASK
2=POST
3=13
4=backup1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=exportDomain
10=IDG-QA-2
11=192.168.72.100
12=5550
13=CarRentA_Domain
14=/data/backups/store/IDG-QA-2/domain/CarRentA_Domain/CarRentA_Domain-export-2017-06-20-19-26-45-229-persisted.zip

Publish Backup Events via Syslog and Email

Setup

1. The maintenance configurable parameters page provides information on how to setup the syslog destination.
2. The Email destination is configured in the plan definition.
3. Configure the SMTP parameters from the System Parameters Page, see the System Parameters List Page for a description of each parameter.
4. If you set a value for "The HTTP Address of the UI" parameter - a link to the DPOD UI will be added to the emails with a shortcut to the relevant plan or task execution results.

The following events will be published via Email and/or syslog (as defined in the backup plan):

Plan Events

Backup Plan Completed Successfully
All backup tasks finished successfully
Syslog Message Id - 0x00a0300a

Backup Plan Completed Successfully with Skipped Tasks
Some backup tasks finished successfully and some were skipped (but none failed)
Syslog Message Id - 0x00a0301a

Backup Plan Failed
At least one task failed
Syslog Message Id - 0x00a0302a

Task Events

Backup Task Completed Successfully
A backup task finished execution, and all files downloaded to the user's storage
Syslog Message ID - 0x00a0100a

Backup Task Failed
A backup task failed for any reason
Syslog Message ID - 0x00a0101a

Backup Task - Found Unsaved Changes in Domain (Export-Domain tasks only)
When unsaved changes are found in the domain, DPOD will create backups for both persisted and non-persisted changes, and a warning message will be issued.
Syslog Message ID - 0x00a0102a

Backup Task Skipped
When a backup task did not execute - e.g. when the device was unavailable
Syslog Message ID - 0x00a0103a

Backup Task Long Running
If a task's status did not change for more than 60 minutes (see maintenance configurable parameters for more information), DPOD will issue the "Long Running" event and will consider the task as finished
Syslog Message ID - 0x00a0104a

Backup Task was not Executed
For tasks that passed all validations but did not execute. E.g. when the maintenance window timeframe ended before the task was executed
Syslog Message ID - 0x00a0105a

Appliance Configuration Synchronization

This section contains information about performing configuration synchronization between domains on your DataPower Appliances.

- Sync Limitations and Notes
- Sync Plan
- Sync Activity
- Sync Execution (Tasks)
- Sync - User Defined Scripts
- Publish Sync Events via Syslog and Email

Sync Limitations and Notes

This page provides important notes and lists limitations of the sync process:

Services on the target domains will be unavailable for a period of a few minutes or more during synchronization.
It is the user's responsibility to reroute traffic to other devices (e.g. by providing pre/post customer supplied scripts).

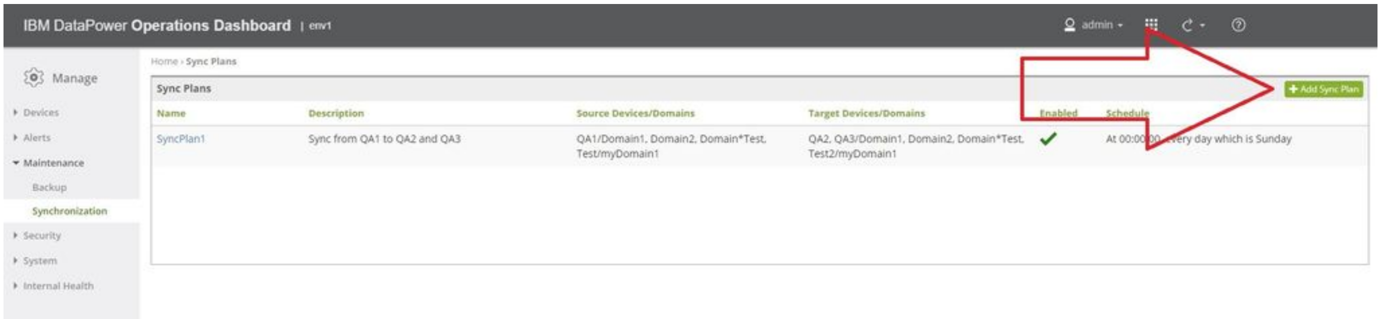
It is the user's responsibility to verify the functionality of the target domain, as failure in synchronization may leave the domain in an inconsistent state.

1. Sync is only supported for devices with firmware levels higher than 7.2.0.0
2. This Sync feature does NOT replace DevOps tools, it is not aimed for promoting configuration from one environment to another
3. This Sync feature will NOT synchronize services in the "default" domain
4. This Sync feature will NOT synchronize API Connect domains
5. It is the user's responsibility to create the target domains; The Sync feature will not create them automatically.
6. This sync feature does NOT support IDG Docker containers
7. This sync feature will only synchronize persisted configuration
8. The target domain will be deleted and no objects will be imported if there are errors in the supplied deployment policy
9. Sync is done on a domain level (entire domains only)
10. This sync feature will NOT synchronize key material (certificates, Kerberos keytabs, etc.)
11. Password map/alias synchronization is available only when both source and target devices have a firmware level of 7.5.2.4 or above and the Password map/alias synchronization is available only when both source and target devices have a firmware level of 7.5.2.4 or above and the passphrase in both source and target match

Sync Plan

A Sync Plan includes general parameters and definitions for the execution of the sync activities.

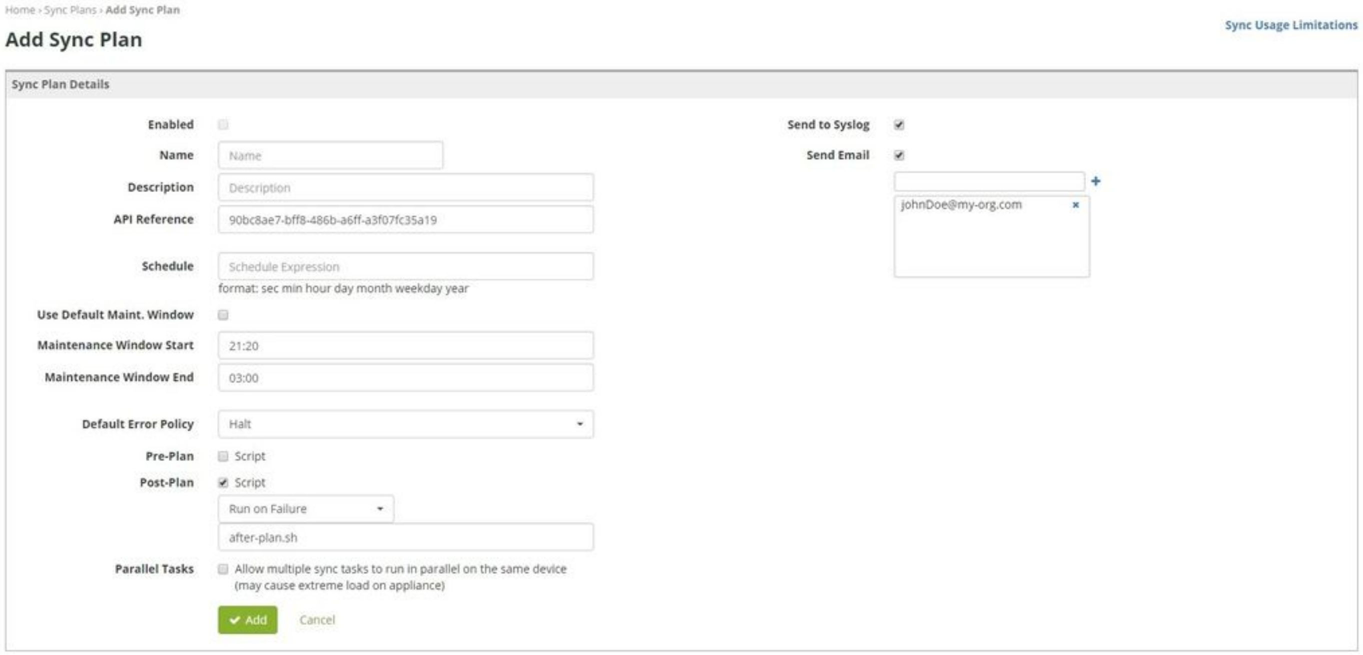
To create a new sync plan, navigate to the Manage MaintenanceSync menu and click on the button to add a new sync plan.



Sync Plans

Name	Description	Source Devices/Domains	Target Devices/Domains	Enabled	Schedule
SyncPlan1	Sync from QA1 to QA2 and QA3	QA1/Domain1, Domain2, Domain*Test, Test/myDomain1	QA2, QA3/Domain1, Domain2, Domain*Test, Test2/myDomain1	✓	At 00:00:00 every day which is Sunday

The system will display the "Add Sync Plan" page. Consult the screenshot and the table below in order to create a new sync plan in the system.



Add Sync Plan

Sync Plan Details

Enabled □
Name: Name
Description: Description
API Reference: 90bc8ae7-bff8-486b-a6ff-a3f07fc35a19
Schedule: Schedule Expression
format: sec min hour day month weekday year
Use Default Maint. Window □
Maintenance Window Start: 21:20
Maintenance Window End: 03:00
Default Error Policy: Halt
Pre-Plan: □ Script
Post-Plan: ☑ Script
Run on Failure
after-plan.sh
Parallel Tasks: □ Allow multiple sync tasks to run in parallel on the same device (may cause extreme load on appliance)

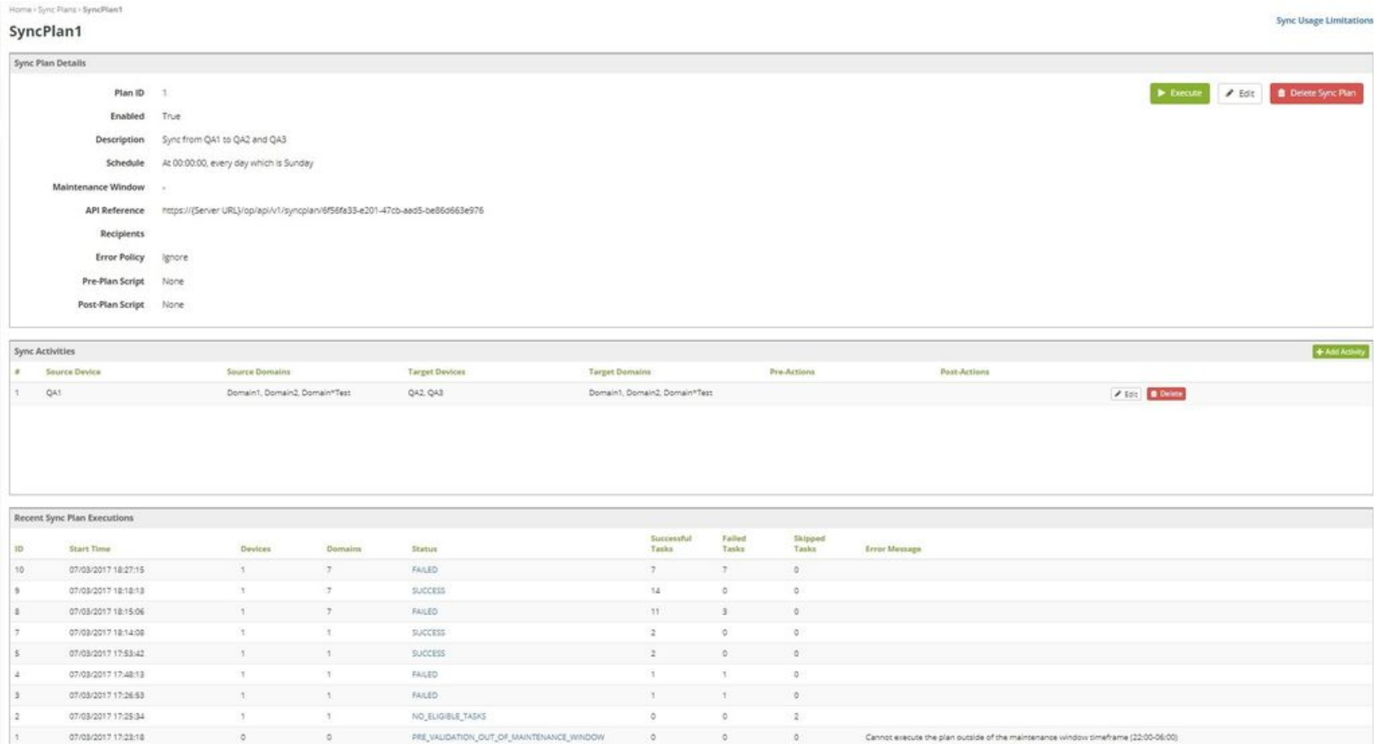
Send to Syslog ☑
Send Email ☑
johnDoe@my-org.com

Attribute	Mandatory?	Description
Enabled	Yes	Only enabled plans may be executed, a plan cannot be enabled if it does not contain any activities
Name	Yes	A user friendly name for the plan, e.g. "SyncQA"
Description	No	A user friendly description for the plan, e.g. "Sync all QA2 device with QA1"
API Reference	Yes	A reference that will be used to execute the plan via the Sync REST API. This field is pre-populated with a unique value generated by DPOD, you may change this value.
Schedule	Yes (only for enabled plans)	When to schedule the sync plan. This field has no effect when the plan is not enabled. Format is identical to the report scheduling format For scheduled executions - DPOD checks if the source domain was changed since the last time it was synced to the target domain. If no changes were detected, the sync will not commence.

Use Default Maint. Window	Yes	Should this plan use the default maintenance window defined for the system parameters. (See maintenance configurable parameters for more information)
Maintenance Window Start	No	When not using the system default maintenance window, this will be used as the plan's maintenance window start time in 24H, HH:MM format (e.g. 21:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)
Maintenance Window End	No	When not using the system default maintenance window, this will be used as the plan's maintenance window end time in 24H, HH:MM format (e.g. 06:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)
Default Error Policy	Yes	**Halt** - when a task failed validation or execution, stop all other tasks waiting for execution from this plan. **Ignore** - when a task failed validation or execution, ignore and continue to run other tasks from this plan.
Pre-Plan Script	No	A user defined script to run before any of the tasks is executed. The script will not run if the plan failed validation, e.g. when it is executed outside the maintenance window timeframe. If the script fails (the return code was greater than 0) - the plan will fail too and its tasks will not be executed. See user defined scripts for more information
Post-Plan Script	No	A user defined script to run after all the tasks finished executing. The screen lets the user select whether to always execute this script or execute only when at least one task failed. See user defined scripts for more information
Parallel Tasks	No	Allow multiple sync tasks to run in parallel on the same device Enabling this feature can cause extreme load on the appliance and may fail the sync process and the running transactions on the device.
Send to Syslog	No	Send syslog messages for events generated by this plan- see publish sync events via syslogs and email
Send Email	No	Send emails for events generated by this plan - see publish sync events via syslogs and email

The Plan Details Page

Click the plan's name on the Sync Plans page to display the Plan's Details Page



SyncPlan1

Sync Plan Details

Plan ID	1
Enabled	True
Description	Sync from QA1 to QA2 and QA3
Schedule	At 00:00:00, every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/syncplan/6f56fa33-e201-47cb-aad5-be86d663e976
Recipients	
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

Sync Activities

#	Source Device	Source Domains	Target Devices	Target Domains	Pre-Actions	Post-Actions
1	QA1	Domain1, Domain2, Domain*Test	QA2, QA3	Domain1, Domain2, Domain*Test		

Recent Sync Plan Executions

ID	Start Time	Devices	Domains	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
10	07/03/2017 18:27:15	1	7	FAILED	7	7	0	
9	07/03/2017 18:18:13	1	7	SUCCESS	14	0	0	
8	07/03/2017 18:15:06	1	7	FAILED	11	3	0	
7	07/03/2017 18:14:08	1	1	SUCCESS	2	0	0	
5	07/03/2017 17:53:42	1	1	SUCCESS	2	0	0	
4	07/03/2017 17:48:13	1	1	FAILED	1	1	0	
3	07/03/2017 17:26:53	1	1	FAILED	1	1	0	
2	07/03/2017 17:25:34	1	1	NO_ELIGIBLE_TASKS	0	0	2	
1	07/03/2017 17:23:18	0	0	PRE_VALIDATION_OUT_OF_MAINTENANCE_WINDOW	0	0	0	Cannot execute the plan outside of the maintenance window timeframe (22:00-06:00)

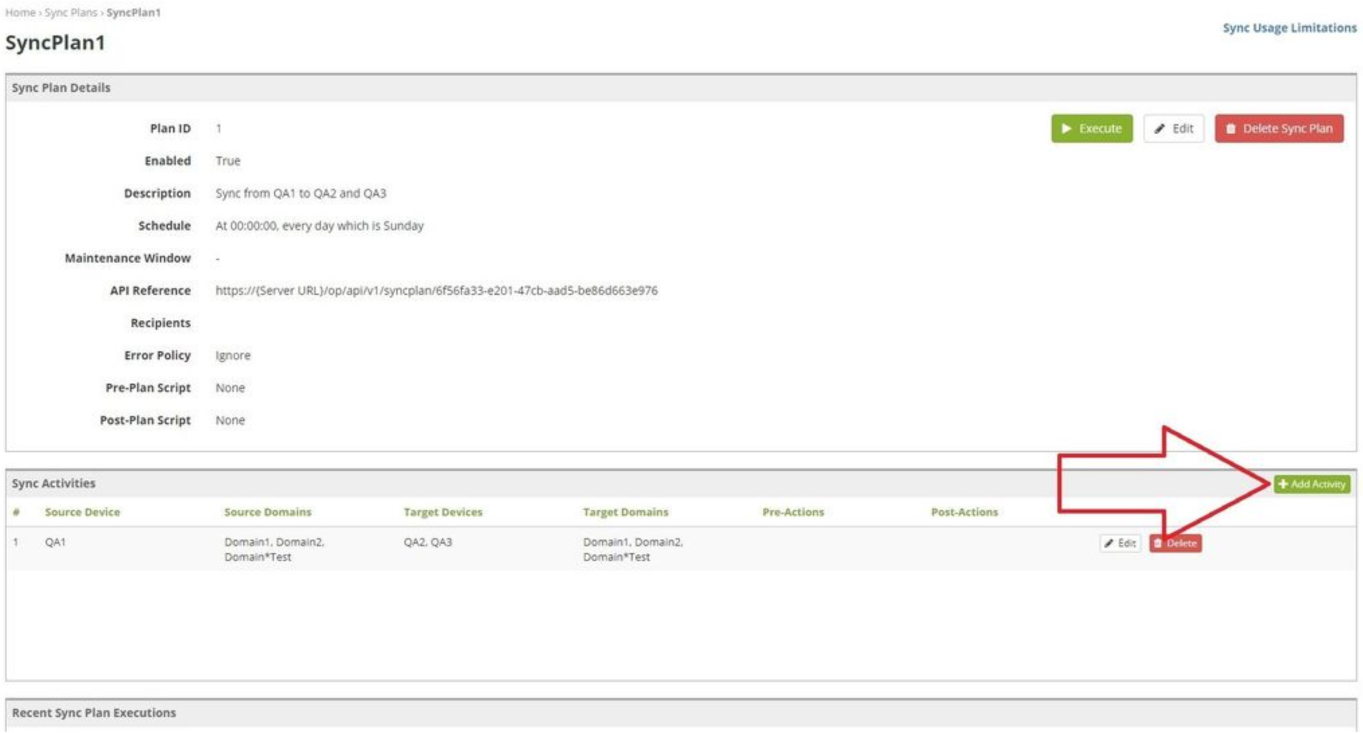
The Plan Details page is composed of three parts:

1. Plan Details - Displays the plan details, and lets the user Edit the plan, Delete it, or execute it in an ad-hoc manner (only for enabled plans)
2. Sync Activities - Add, Edit or Delete a sync activity
3. Recent Sync Plan Executions - Displays results for the most recent 40 executions of the plan - see Maintenance Plans Status Description for descriptions of the possible plan statuses

Sync Activity

A Sync Activity defines the target and the destination domains to be synced, pre/post actions and the error policy to use.

To add a new sync activity, navigate to Mange Maintenance Sync, select the plan to add an activity to and click "Add Activity" from the Sync Plan Details Page.



Sync Plan Details

Plan ID	1
Enabled	True
Description	Sync from QA1 to QA2 and QA3
Schedule	At 00:00:00, every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/syncplan/6f56fa33-e201-47cb-aad5-be86d663e976
Recipients	
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

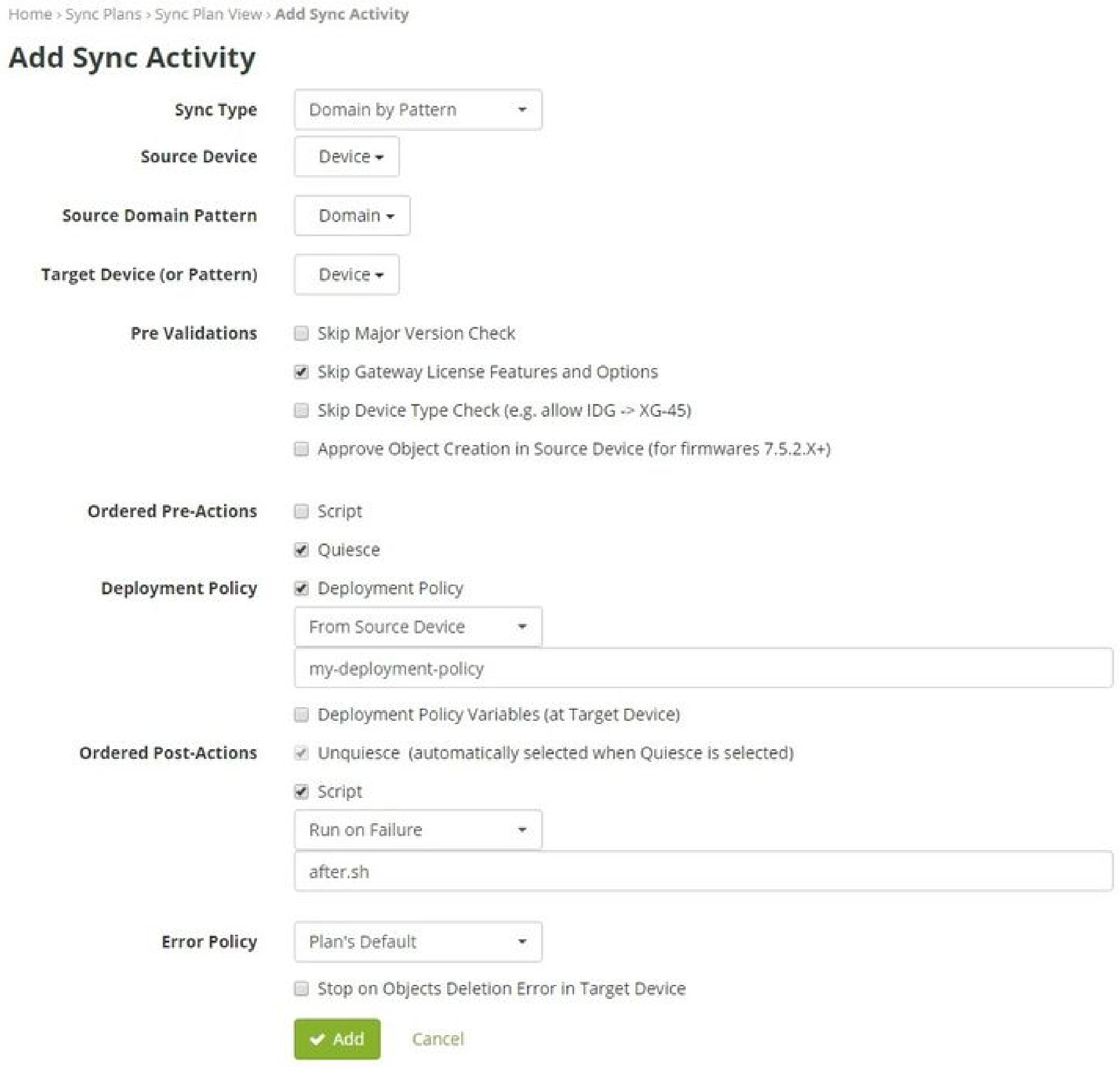
Sync Activities

#	Source Device	Source Domains	Target Devices	Target Domains	Pre-Actions	Post-Actions
1	QA1	Domain1, Domain2, Domain*Test	QA2, QA3	Domain1, Domain2, Domain*Test		

Recent Sync Plan Executions

e

The system will display the "Add Sync Activity" page. Consult the screenshot and the table below in order to create a new sync activity in the system.



Home › Sync Plans › Sync Plan View › **Add Sync Activity**

Add Sync Activity

Sync Type	Domain by Pattern
Source Device	Device
Source Domain Pattern	Domain
Target Device (or Pattern)	Device
Pre Validations	□ Skip Major Version Check ☑ Skip Gateway License Features and Options □ Skip Device Type Check (e.g. allow IDG -> XG-45) □ Approve Object Creation in Source Device (for firmwares 7.5.2.X+)
Ordered Pre-Actions	□ Script ☑ Quiesce
Deployment Policy	☑ Deployment Policy From Source Device my-deployment-policy □ Deployment Policy Variables (at Target Device)
Ordered Post-Actions	☑ Unquiesce (automatically selected when Quiesce is selected) ☑ Script Run on Failure after.sh
Error Policy	Plan's Default □ Stop on Objects Deletion Error in Target Device

Sync Types

There are 3 types of destination/target pairs:

> For all sync types - DPOD will NOT create any domains on the target devices, it is the admin's responsibility to create them.
> If a target domain does not exist - the sync task will be skipped

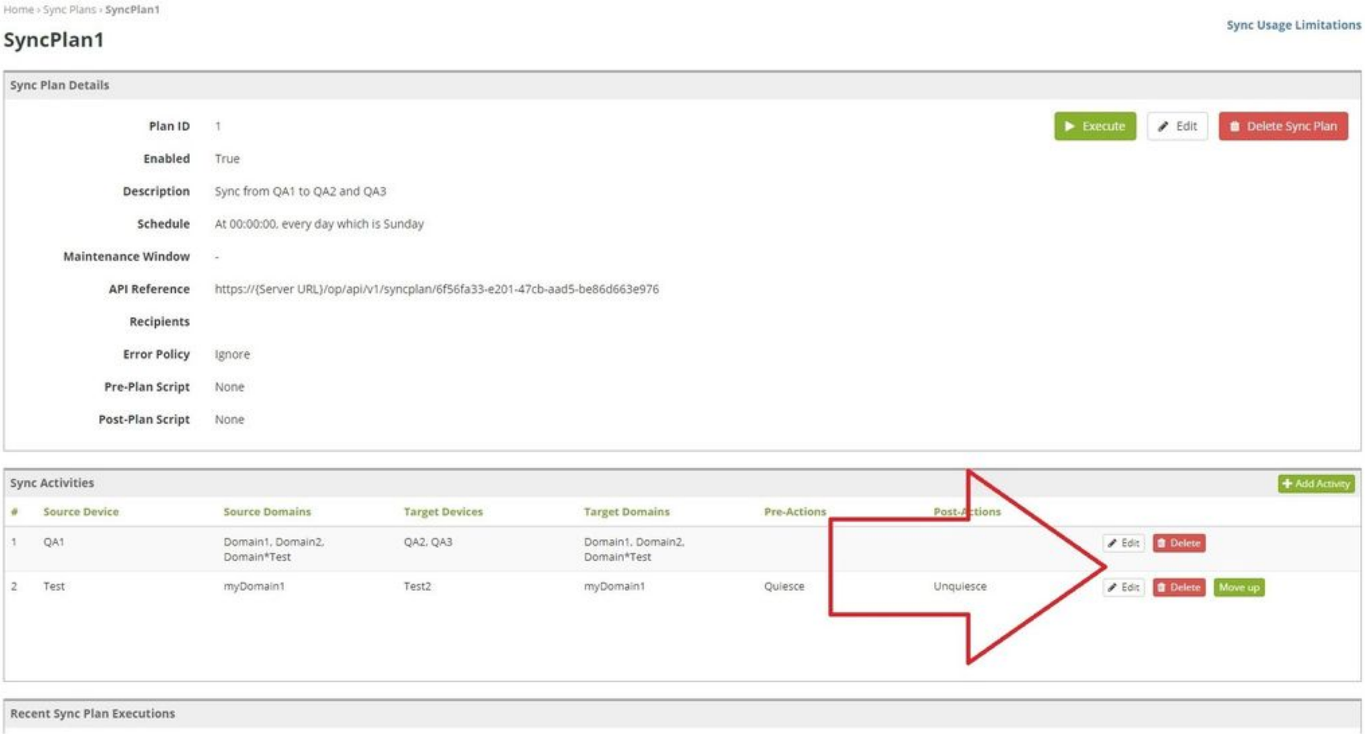
1. **Domain Pattern** - Enter source device name, source domain pattern and target device pattern.
   All the source domains matching the pattern will be synced to domains with identical names on the target device(s)
   For example:
   Source Device = QA1, Source Domain = Domain*, Target Device = QA2, QA3
   Results - the domain QA1/Domain1 will be synced to QA2/Domain1 and QA3/Domain1
   the domain QA1/Domain2 will be synced to QA2/Domain2 and to QA3/Domain3
2. **Single Domain** - Enter source device and domain names (no patterns) and the target device pattern and target domain name
   This will sync a single domain from the source to the same or different domain name on the target device(s)
   For example:
   Source Device = QA1, Source Domain = Domain1, Target Device = QA2, QA3, Target Domain = CopyDomain1
   Results - The domain QA1/Domain1 will be synced to QA2/CopyDomain1 and to QA3/CopyDomain1
3. **Device** - Enter source device name and a target device pattern, all the domains from the source device will be synced to the target device(s)
   For Example:
   Source Device = PROD1, Target Device = DRP*

Results - All the domains from device PROD1 will be synced to devices DRP_Active and DRP_Inactive

Attribute	Mandatory?	Description
Sync Type	Yes	Domain Pattern, Single Domain or Device as explained above
Pre Validation - Skip Major Version Check	Yes	Select to allow Syncing configuration from higher firmware major release (e.g. 7.5.2.0) to lower major release (e.g. 7.2.0.0) Syncing from higher firmware major release to lower major release may cause features that were introduced in the later version not to work.
Pre Validations - Skip Gateway License Features and Options	Yes	Select to allow Syncing configuration between devices with non-identical licenses (e.g. the source device has B2B or SQL-ODBC license and the target device does not)
Pre Validations - Skip Device Type Check	Yes	Select to allow Syncing configuration between higher device types to lower device types (e.g. IDG to XG-45 or XI-52 to XG-45)
Approve Object Creation in Source Device	Yes	When both source and target devices firmware versions are 7.5.2.X+ In order to test that the password map alias in the source and target are identical - DPOD will need approval to create a temporary object in the source device
Pre-Action Script	No	A user defined script to run before the task is executed. The task will not be executed If the script fails (the return code was greater than 0) See user defined scripts for more information
Pre-Action Quiesce	No	Should the device(s) be quiesced before the sync is executed. The timeout value that is passed to the quiesce SOMA is controlled by a system parameter (see maintenance configurable parameters for more information)
Deployment Policy	No	An optional deployment policy from the source or target device, if the object is not found on the device, the sync task will not execute
Deployment Policy Variables	No	An optional deployment policy variables object on the target device, if the object is not found on the target device, the sync task will not execute
Post-Action Unquiesce	No	This option cannot be edited - it will be automatically set to the value of the Pre-Action Quiesce. The user may set how long DPOD waits for the unquiesce operation to finish before cancelling the task via a system parameter (see maintenance configurable parameters for more information)
Post-Action Script	No	A user defined script to run after the task is executed. The user selects whether the script should run always when a task completes, or only when the task execution fails. See user defined scripts for more information
Error Policy	Yes	Select how this backup activity handles errors. **Plan's Default** - Use the value that was set for the plan **Halt** - When the task failed validation or execution, stop all other tasks from this plan that are waiting for execution **Ignore** - When the task failed validation or execution, ignore and continue to run other tasks from this plan
Stop on Objects Deletion Error in Target Device	Yes	Before importing the object to the target domain, DPOD will first delete objects from the target domain - check this option to stop the import if deletion of those objects failed

Edit, Delete or Reorder Activities

The Sync Plan Details Page allows the user to edit, delete or reorder activities.
When the plan is scheduled to run, the activities will be processed in the order they were defined (see Sync Execution for more information)



SyncPlan1

Sync Plan Details

Plan ID	1
Enabled	True
Description	Sync from QA1 to QA2 and QA3
Schedule	At 00:00:00. every day which is Sunday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/syncplan/6f56fa33-e201-47cb-aad5-be86d663e976
Recipients	
Error Policy	Ignore
Pre-Plan Script	None
Post-Plan Script	None

Sync Activities

#	Source Device	Source Domains	Target Devices	Target Domains	Pre-Actions	Post-Actions
1	QA1	Domain1, Domain2, Domain*Test	QA2, QA3	Domain1, Domain2, Domain*Test		
2	Test	myDomain1	Test2	myDomain1	Quiesce	Unquiesce

Recent Sync Plan Executions

Sync Execution (Tasks)

This page describes how DPOD prepares the execution flow of a sync plan (using tasks) and subsequently - how the tasks themselves are executed

Task Creation Flow

General execution flow for a sync plan:

1. Verify that the system allows Syncs to run. (See Configurable Parameters and Settings to learn how to enable or disable all sync activities)
2. Verify that the current system time is within the maintenance window timeframe defined for the plan
3. Iterate over all the activities defined for the plan, and split them into executable tasks.
   For example: consider a plan with two activities, one to sync device PROD1 to DR1 and a second to sync domain pattern with source device = PROD1, source domain = Flight* and target device = PROD2
   DPOD will create eight tasks:
   a. Export task for source device/domain PROD1/Domain1
   b. Import task for target device/domain DR1/Domain1
   c. Import task for target device/domain DR1/Domain2
   d. Import task for target device/domain DR1/Domain3
   e. Export task for source device/domain PROD1/Flight1
   f. Import task for target device/domain PROD2/Flight1
   g. Export task for source device/domain PROD1/Flight2
   h. Import task for target device/domain PROD2/Flight2
4. If all the created tasks are in "Skipped" state (because the devices are not available, or because no devices or domains matched the input patterns) - the plan will stop
5. If there are any tasks waiting to be executed - the Pre-Plan Script will be executed (if requested in the plan settings). The plan will stop if the script's return code is larger than 0.

Task Execution Flow

After the sync tasks are created, they will start to execute. The following is the general execution flow for a sync task:

> Sync tasks will start to execute in the order they were created, which corresponds to the order which the activities are defined.
> Two different tasks will not execute concurrent syncs on the same device, unless the option "Allow multiple sync tasks to run in parallel" was checked in the plan definition

1. Verify that the current system time is within the maintenance window timeframe defined for the plan.
2. Verify that both source and target devices' firmware levels are above 7.1.0.0
3. If a deployment policy was specified in the sync activity definition - ensure it exists
4. If a deployment policy variables object was specified in the sync activity definition - ensure it exists
5. Check that the source and target device type match (IDG > XB-62 > XI-52 > XG-45) - you can turn this check off in the sync activity definition
6. Check that the source device major firmware level is lower or equal to the target device major firmware level - you can turn this check off in the sync activity definition
7. Check that the target device contains the same licenses/features of the source device (e.g. B2B, SQL-ODBC, Tibco-ESM) - you can turn this check off in the sync activity definition
8. If both source and target devices have firmware level above 7.5.2.4, DPOD will try to check if the passphrase in both source and target match, and will stop the sync process if they do not.
   If one of the source or target devices' firmware is below level 7.5.2.4, DPOD will not sync any password map/alias objects
9. Export the source domain's configuration
10. If pre-quiesce was requested - check that the domain is not already quiesced
11. Run the user's pre-script (if requested in the activity), the task will stop if the script return value is larger than 0
12. Issue a Quiesce domain/device SOMA (if requested in the activity)
13. Wait for the device or domain to finish quiescing. A timeout value may be specified for the Quiesce SOMA (see Configurable Parameters and Settings),
    DPOD will cancel the task if the domain(s) are not yet quiesced 3 minutes after the specified timeout, and will issue an Unquiesce SOMA
14. Perform an Import Dry-run to try and detect any errors before the actual Import
15. Delete objects on the target domain (DPOD does not use "reset domain" in order to retain the passwords on the target domains) -
    The following object types will be deleted:
    a. WSGateway
    b. MultiProtocolGateway
    c. XMLFirewallService
    d. SSLProxyService
    e. HTTPService
    f. B2BGateway
    g. TCPProxyService
    h. WebTokenService
    i. WebAppFW

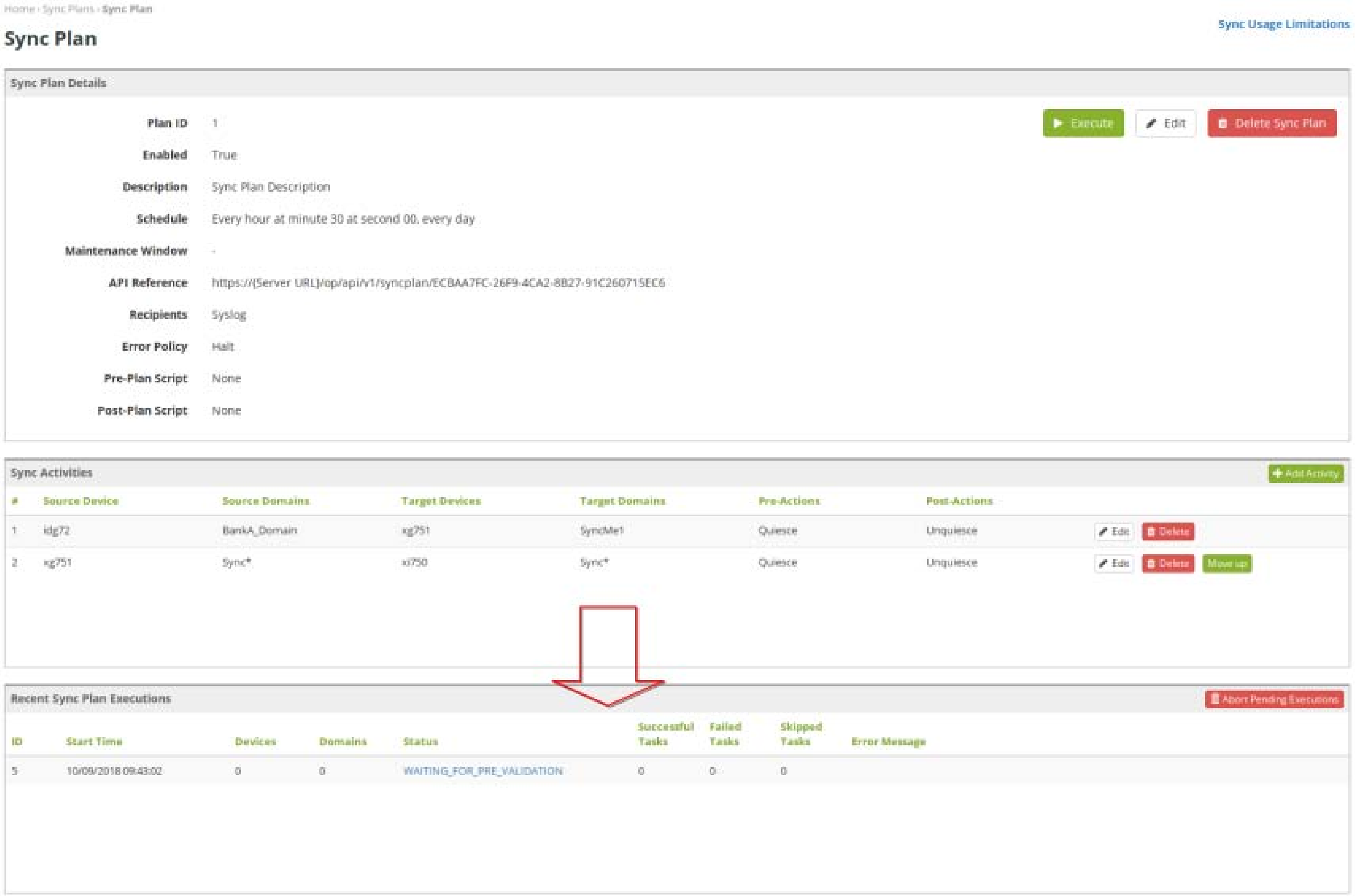
j. XSLProxyService
k. CloudGatewayService
l. SQLDataSource
m. MQQMGroup
n. MQQM
o. ISAMReverseProxy
p. TibcoEMSServer
q. LoadBalancerGroup
r. WebSphereJMSServer

16. Import the configuration into the target domain
17. Save config on the target domain
18. Unquiesce the device/domain (if it was previously quiesced by this task)
19. Wait for the device/domain to unquiesce. A timeout value may be specified for this operation. 3 minutes after the timeout, DPOD will stop waiting for the unquiesce operation and will fail the task (the device's unquiesce operation will not be interrupted though)
20. Run the user's post-task script (if requested in the activity)

When all the plan's tasks completed execution, the post-plan script will be executed (if requested in the plan settings).

Sync Execution Results

The Plan Details page shows the 40 most recent plan execution results



Sync Plan

Sync Plan Details

Plan ID	1
Enabled	True
Description	Sync Plan Description
Schedule	Every hour at minute 30 at second 00, every day
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/syncplan/ECBAA7FC-26F9-4CA2-8B27-91C260715EC6
Recipients	Syslog
Error Policy	Halt
Pre-Plan Script	None
Post-Plan Script	None

Sync Activities

#	Source Device	Source Domains	Target Devices	Target Domains	Pre-Actions	Post-Actions
1	idg72	BankA_Domain	xg751	SyncMe1	Quiesce	Unquiesce
2	xg751	Sync*	xi750	Sync*	Quiesce	Unquiesce

Recent Sync Plan Executions

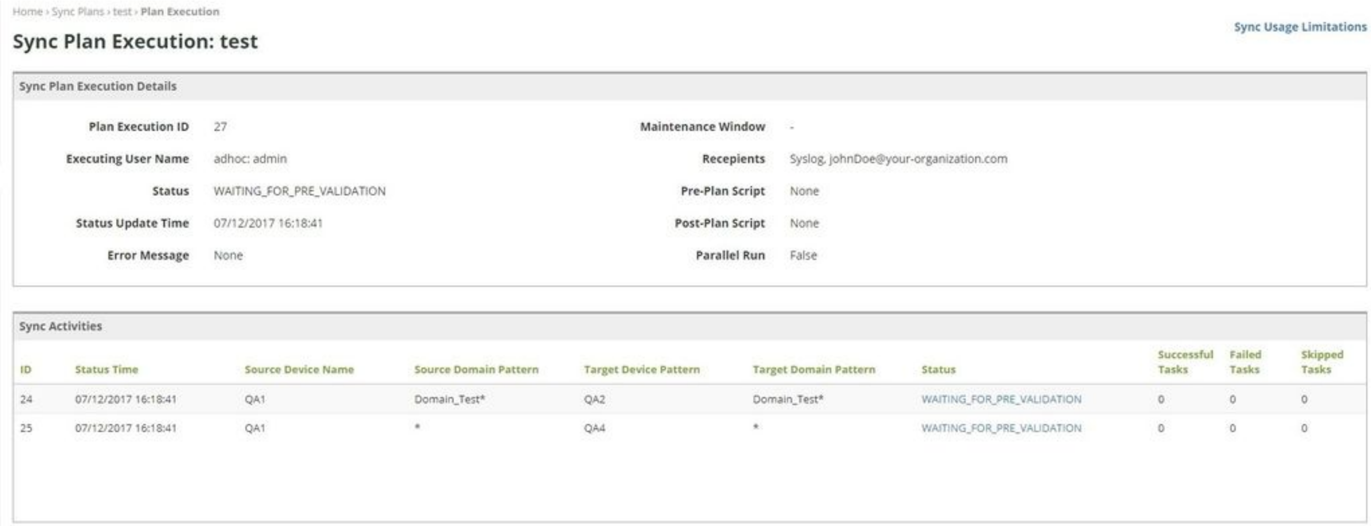
ID	Start Time	Devices	Domains	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
5	10/09/2018 09:43:02	0	0	WAITING_FOR_PRE_VALIDATION	0	0	0	

The following table outlines the details for each column in the plan execution table

Column Name	Description
ID	The Plan Execution ID
Start Time	The time the plan entered the execution queue
Devices	Number of devices that were supposed to be synced. Both failed and successful syncs are aggregated.

Domains	Number of domains that were supposed to be synced. Both failed and successful syncs are aggregated.
Status	The current status of the plan
Successful Tasks	Number of sync tasks that completed successfully for this plan execution
Failed Tasks	Number of sync tasks that failed for this plan execution
Skipped Tasks	Number of sync tasks that did not execute, e.g. because the device was not available
Error Message	Plan's Error message (If any)

*Click the red "Abort Pending Executions" to stop execution in status "WAITING_FOR_PRE_VALIDATION" that did not started yet.
**Click the status column to drill into the plan execution details page.



Sync Plan Execution: test

Sync Plan Execution Details

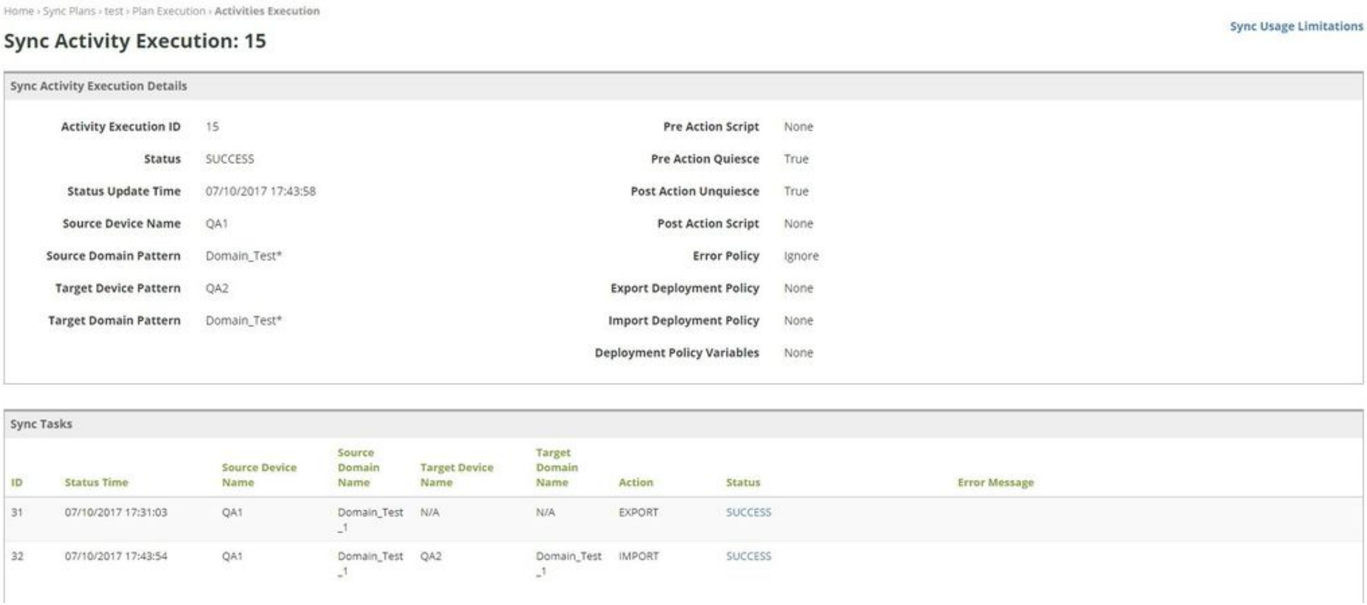
Plan Execution ID	27	Maintenance Window	-
Executing User Name	adhoc: admin	Recepients	Syslog, johnDoe@your-organization.com
Status	WAITING_FOR_PRE_VALIDATION	Pre-Plan Script	None
Status Update Time	07/12/2017 16:18:41	Post-Plan Script	None
Error Message	None	Parallel Run	False

Sync Activities

ID	Status Time	Source Device Name	Source Domain Pattern	Target Device Pattern	Target Domain Pattern	Status	Successful Tasks	Failed Tasks	Skipped Tasks
24	07/12/2017 16:18:41	QA1	Domain_Test*	QA2	Domain_Test*	WAITING_FOR_PRE_VALIDATION	0	0	0
25	07/12/2017 16:18:41	QA1	*	QA4	*	WAITING_FOR_PRE_VALIDATION	0	0	0

Column Name	Description
ID	The Activity Execution ID
Status Time	The last time the status of the activity changed
Source Device Name	The source device name
Source Domain Pattern	The source domain name or pattern
Target Device Pattern	The target device name or pattern
Target Domain Pattern	The target domain name or pattern
Status	The current status of the activity
Successful Tasks	Number of backup tasks that completed successfully for this activity execution
Failed Tasks	Number of backup tasks that failed for this activity execution
Skipped Tasks	Number of backup tasks that were skipped for this activity execution

Click the status column to drill into the activity execution details page



Home › Sync Plans › test › Plan Execution › Activities Execution

Sync Usage Limitations

Sync Activity Execution: 15

Sync Activity Execution Details

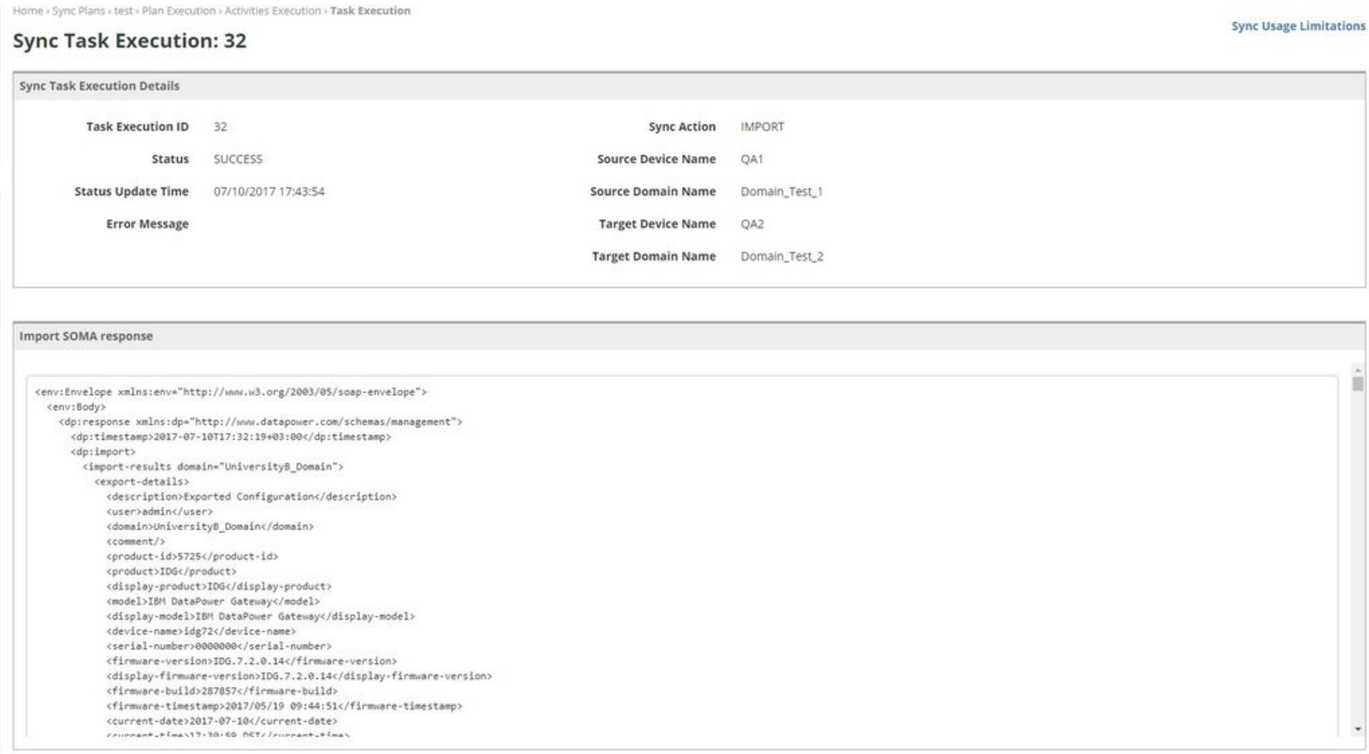
Activity Execution ID	15	Pre Action Script	None
Status	SUCCESS	Pre Action Quiesce	True
Status Update Time	07/10/2017 17:43:58	Post Action Unquiesce	True
Source Device Name	QA1	Post Action Script	None
Source Domain Pattern	Domain_Test*	Error Policy	Ignore
Target Device Pattern	QA2	Export Deployment Policy	None
Target Domain Pattern	Domain_Test*	Import Deployment Policy	None
		Deployment Policy Variables	None

Sync Tasks

ID	Status Time	Source Device Name	Source Domain Name	Target Device Name	Target Domain Name	Action	Status	Error Message
31	07/10/2017 17:31:03	QA1	Domain_Test_1	N/A	N/A	EXPORT	SUCCESS	
32	07/10/2017 17:43:54	QA1	Domain_Test_1	QA2	Domain_Test_1	IMPORT	SUCCESS	

Column Name	Description
ID	The Task Execution ID
Status Time	The last time the status of the task changed
Source Device Name	The source device name
Source Domain Name	The source domain name
Target Device Name	The target device name
Target Domain Name	The target domain name
Action	EXPORT or IMPORT
Status	The current status of the task
Error Message	Task's Error message if any

Click the status column to drill into the task execution results page, this page will display the Import SOMA result for the task (if an Import was actually performed)



Home › Sync Plans › test › Plan Execution › Activities Execution › Task Execution
Sync Usage Limitations

Sync Task Execution: 32

Sync Task Execution Details

Task Execution ID	32	**Sync Action**	IMPORT
Status	SUCCESS	**Source Device Name**	QA1
Status Update Time	07/10/2017 17:43:54	**Source Domain Name**	Domain_Test_1
Error Message		**Target Device Name**	QA2
		Target Domain Name	Domain_Test_2

Import SOMA response

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Body>
    <dp:response xmlns:dp="http://www.datapower.com/schemas/management">
      <dp:timestamp>2017-07-10T17:32:19+03:00</dp:timestamp>
      <dp:import>
        <import-results domain="UniversityB_Domain">
          <export-details>
            <description>Exported Configuration</description>
            <user>admin</user>
            <domain>UniversityB_Domain</domain>
            <comment/>
            <product-id>5725</product-id>
            <product>IDG</product>
            <display-product>IDG</display-product>
            <model>IBM DataPower Gateway</model>
            <display-model>IBM DataPower Gateway</display-model>
            <device-name>idg72</device-name>
            <serial-number>0000000</serial-number>
            <firmware-version>IDG.7.2.0.14</firmware-version>
            <display-firmware-version>IDG.7.2.0.14</display-firmware-version>
            <firmware-build>287857</firmware-build>
            <firmware-timestamp>2017/05/19 09:44:51</firmware-timestamp>
            <current-date>2017-07-10</current-date>
            <current-time>17:30:59 DST</current-time>
```

Sync - User Defined Scripts

DPOD allows execution of user defined, custom scripts before and after both Plan and Task execution.
The scripts are executed from /app/custom/scripts (See Configurable Parameters and Settings for information on how to change this path)

Any script that returns a return code larger than 0 is considered to have failed.

> if a pre-plan or a pre-task script failed - the plan or task will be flagged as failed and will **not** execute.
> If a pre-task script failed, the post-task script will still be executed (if requested)

DPOD will send certain parameters to the script, to indicate the execution details and completion status.

Parameters Sent to the Sync Pre-Plan Script

Sample script: /app/custom/scripts/sync_pre_plan_sample.sh

1=PLAN_TYPE - The constant "SYNC-PLAN"
2=PLAN_STAGE - The constant "PRE"
3=PLAN_ID - The ID of the sync plan
3=PLAN_NAME - The name of the sync plan

Example:
1=SYNC-PLAN
2=PRE
3=16
4=sync1

Parameters Sent to the Sync Post-Plan Script

Sample script: /app/custom/scripts/sync_post_plan_sample.sh

1=PLAN_TYPE - The constant "SYNC-PLAN"
2=PLAN_STAGE - The constant "POST"
3=PLAN_ID - The ID of the sync plan
4=PLAN_NAME - The name of the sync plan
5=FINAL_STATUS_CODE - Final status code of the sync plan
6=FINAL_ERROR_MSG - Final error message of the sync plan, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=TASKS_VALUES - list of comma separated values for each task- task ID, sync action (EXPORT or IMPORT), source device, source domain, target device, target domain, task status - different tasks are separated with ~ (Tilde sign)

Example:
1=SYNC-PLAN
2=POST
3=16
4=sync test 1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=13,EXPORT,QA1,Domain1,NONE,NONE,SUCCESS~14,IMPORT,QA1,Domain1,QA2,Domain1,SUCCESS

Parameters Sent to the Sync Pre-Task Script

Sample script: /app/custom/scripts/sync_pre_task_sample.sh

1=TASK_TYPE - The constant "SYNC-TASK"
2=TASK_STAGE - The constant "PRE"
3=TASK_ID - The ID of the sync task
4=PLAN_NAME - The name of the sync plan that generated this task
5=SYNC_ACTION - EXPORT or IMPRT
6=SOURCE_DEVICE_NAME - The source device name
7=SOURCE_DEVICE_HOST - The source device host
8=SOURCE_SOMA_PORT - The soma port of the source device
9=SOURCE_DOMAIN - The source domain name
10=TARGET_DEVICE_NAME - The target device name (or NONE if the task is an EXPORT task)
11=TARGET_DEVICE_HOST - The target device host (or NONE if the task is an EXPORT task)
12=TARGET_SOMA_PORT - The soma port of the target device (or NONE if the task is an EXPORT task)

13=TARGET_DOMAIN - The target domain name (or NONE if the task is an EXPORT task)

Example:
1=SYNC-TASK
2=PRE
3=12
4=sync test 1
5=IMPORT
6=QA1
7=192.168.72.100
8=5550
9=Domain1
10=QA2
11=192.168.72.105
12=5550
13=Domain1

Parameters Sent to the Sync Post-Task Script

Sample script: /app/custom/scripts/sync_post_task_sample.sh

1=TASK_TYPE - The constant "SYNC-TASK"
2=TASK_STAGE - The constant "POST"
3=TASK_ID - The ID of the sync task
4=PLAN_NAME - The name of the sync plan that generated this task
5=FINAL_STATUS - Final status code of the sync task
6=FINAL_ERROR_MSG - Final error message of the sync task, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=SYNC_ACTION - EXPORT or IMPORT
10=SOURCE_DEVICE_NAME - The source device name
11=SOURCE_DEVICE_HOST - The source device host
12=SOURCE_SOMA_PORT - The soma port of the source device
13=SOURCE_DOMAIN - The source domain name
14=TARGET_DEVICE_NAME - The target device name (or NONE if the task is an EXPORT task)
15=TARGET_DEVICE_HOST - The target device host (or NONE if the task is an EXPORT task)
16=TARGET_SOMA_PORT - The soma port of the target device (or NONE if the task is an EXPORT task)
17=TARGET_DOMAIN - The target domain name (or NONE if the task is an EXPORT task)

Example:
1=SYNC-TASK
2=POST
3=13
4=Sync test 1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=IMPORT
10=QA1
11=192.168.72.100
12=5550
13=Domain1
14=QA2
15=192.168.72.105
16=5550
17=Domain1

Publish Sync Events via Syslog and Email

Setup

1. The maintenance configurable parameters page provides information on how to setup the syslog destination.
2. The Email destination is configured in the plan definition.
3. Configure the SMTP parameters from the System Parameters Page, see the System Parameters List Page for a description of each parameter
4. If you set a value for "The HTTP Address of the UI" parameter - a link to the DPOD UI will be added to the emails with a shortcut to the relevant plan or task execution results.

The following events will be published via Email and/or syslog (as defined in the sync plan):

Plan Events

Sync Plan Completed Successfully
All sync tasks finished successfully
Syslog Message Id - 0x00a0400a

Sync Plan Completed Successfully with Skipped Tasks
Some sync tasks finished successfully and some were skipped (but none failed)
Syslog Message Id - 0x00a0401a

Sync Plan Failed
At least one task failed
Syslog Message Id - 0x00a0402a

Task Events

Sync Task Completed Successfully
A sync task finished execution successfully
Syslog Message ID - 0x00a0200a

Sync Task Failed
A sync task failed for any reason
Syslog Message ID - 0x00a0201a

Sync Task - Found Unsaved Changes in Source Domain
A warning message about unsaved changes found in the source domain
Syslog Message ID - 0x00a0202a

Sync Task Skipped
When a sync task did not execute - for example, when the device was not available
Syslog Message ID - 0x00a0203a

Sync Task Long Running
If a task's status did not change for more than 60 minutes (see maintenance configurable parameters for more information), DPOD will issue the "Long Running" event and will consider the task as finished
Syslog Message ID - 0x00a0204a

Sync Task was not Executed
For tasks that passed all validations but did not execute. e.g. when the maintenance window timeframe ended before the task was executed
Syslog Message ID - 0x00a0205a

Appliance Firmware Upgrade

This section contains information about performing firmware upgrade for your DataPower appliances.

- Firmware Upgrade Limitations and Notes
- Firmware Upgrade Plan
- Firmware Upgrade Activity
- Firmware Upgrade Execution (Tasks)
- Firmware Upgrade - User Defined Scripts
- Publish Firmware Upgrade Events via Syslog and Email

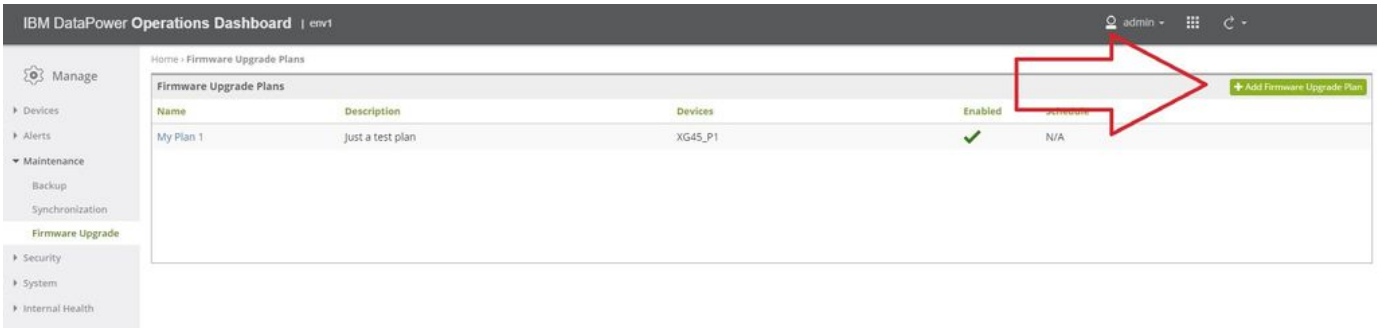
Firmware Upgrade Limitations and Notes

1. Firmware upgrade plan is available for devices with current firmware version of **7.5.x** and above.
2. Firmware upgrade plan will cause downtime to the devices that are being upgraded.
3. Full backup of the system is recommended prior to the upgrade.
4. Make sure there is enough free space in the encrypted and temporary file systems, each file system with at least the size of the upgrade file.
5. This system does not provide rollback functionality. Please use DataPower's web-gui to rollback the firmware if needed.
6. Any special characters at the end of the firmware version string will be ignored (for example, 7.5.2.1zz will be treated as 7.5.2.1). This means that upgrading from version 7.5.2.1zz to version 7.5.2.1 will not be allowed, because they will be considered as the same version.
7. The firmware upgrade process does not support DataPower on Docker or on any other Linux packaging (scrypt only files).
8. Bi-directional SSH connection to each upgraded device is required using the default SSH port (22).
9. This version does not support upgrading devices with tenant feature enabled.

Firmware Upgrade Plan

A Firmware Upgrade Plan includes general parameters and definitions for the execution of the upgrade activities.

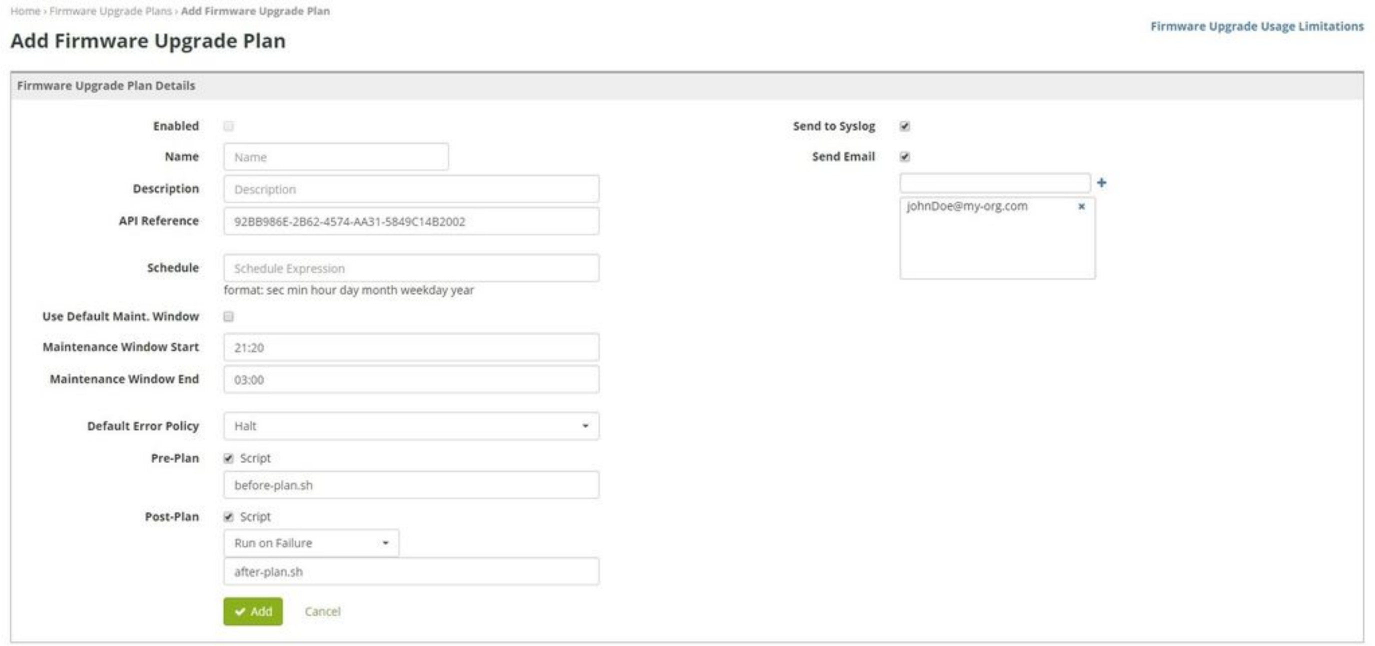
To create a new firmware upgrade plan, navigate to the Manage MaintenanceFirmware Upgrade menu and click on the button to add a new plan.



Firmware Upgrade Plans

Name	Description	Devices	Enabled	Schedule
My Plan 1	Just a test plan	XG45_P1	✓	N/A

The system will display the "Add Firmware Upgrade Plan" page. Consult the screenshot and the table below in order to create a new firmware upgrade plan in the system.


Home › Firmware Upgrade Plans › Add Firmware Upgrade Plan
Firmware Upgrade Usage Limitations
+
×
✔ Add
Cancel

Add Firmware Upgrade Plan

Firmware Upgrade Plan Details

Enabled ☐
Name: Name
Description: Description
API Reference: 92BB986E-2B62-4574-AA31-5849C14B2002
Schedule: Schedule Expression
format: sec min hour day month weekday year
Use Default Maint. Window ☐
Maintenance Window Start: 21:20
Maintenance Window End: 03:00
Default Error Policy: Halt
Pre-Plan: ☑ Script
before-plan.sh
Post-Plan: ☑ Script
Run on Failure
after-plan.sh

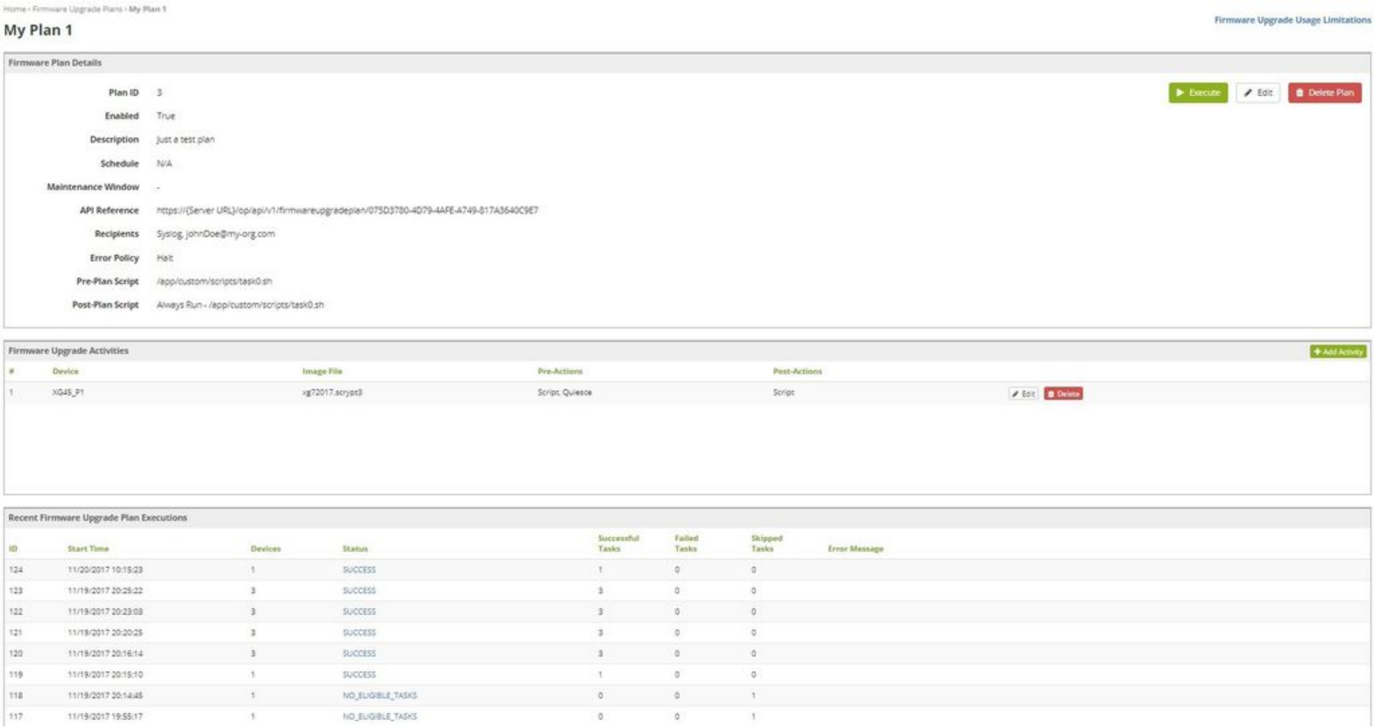
Send to Syslog ☑
Send Email ☑
johnDoe@my-org.com

Attribute	Mandatory?	Description
Enabled	Yes	Only enabled plans may be executed, a plan cannot be enabled if it does not contain any activities
Name	Yes	A user friendly name for the plan, e.g. "UpgradeQA"
Description	No	A user friendly description for the plan, e.g. "Upgrade all QA devices to IDG7.5.1.2"
API Reference	Yes	A reference that will be used to execute the plan via the Firmware Upgrade REST API. This field is pre-populated with a unique value generated by DPOD, you may change this value.
Schedule	No	When to schedule the plan. This field has no effect when the plan is not enabled. Format is identical to the report scheduling format
Use Default Maint. Window	Yes	Should this plan use the default maintenance window defined for the system parameters. (See maintenance configurable parameters for more information)
Maintenance Window Start	No	When not using the system default maintenance window, this will be used as the plan's maintenance window start time in 24H, HH:MM format (e.g. 21:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)

Maintenance Window End	No	When not using the system default maintenance window, this will be used as the plan's maintenance window end time in 24H, HH:MM format (e.g. 06:30) Leave the maintenance window start and end fields empty to disable the maintenance window check (the plan will always be eligible to run)
Default Error Policy	Yes	**Halt** - when a task failed validation or execution, stop all other tasks waiting for execution from this plan. **Ignore** - when a task failed validation or execution, ignore and continue to run other tasks from this plan.
Pre-Plan Script	No	A user defined script to run before any of the tasks is executed. The script will not run if the plan failed validation, e.g. when it is executed outside the maintenance window timeframe. If the script fails (the return code was greater than 0) - the plan will fail too and its tasks will not be executed. See user defined scripts for more information
Post-Plan Script	No	A user defined script to run after all the tasks finished executing. The screen lets the user select whether to always execute this script or execute only when at least one task failed. See user defined scripts for more information
Send to Syslog	No	Send syslog messages for events generated by this plan- see publish firmware upgrade events via syslogs and email
Send Email	No	Send emails for events generated by this plan - see publish firmware upgrade events via syslogs and email

The Plan Details Page

Click the plan's name on the Firmware Upgrade Plans page to display the Plan's Details Page


Home › Firmware Upgrade Plans › My Plan 1
Firmware Upgrade Usage Limitations
▶ Execute
✎ Edit
Delete Plan
+ Add Activity
✎ Edit
Delete

My Plan 1

Firmware Plan Details

Plan ID	3
Enabled	True
Description	Just a test plan
Schedule	N/A
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/firmwareupgradeplan/075D3780-4D79-4AFE-A749-817A3640C9E7
Recipients	Syslog, johnDoe@my-org.com
Error Policy	Halt
Pre-Plan Script	/app/custom/scripts/task0.sh
Post-Plan Script	Always Run - /app/custom/scripts/task0.sh

Firmware Upgrade Activities

#	Device	Image File	Pre-Actions	Post-Actions
1	XG45_P1	xg72017.scrypt3	Script, Quiesce	Script

Recent Firmware Upgrade Plan Executions

ID	Start Time	Devices	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
124	11/20/2017 10:15:23	1	SUCCESS	1	0	0	
123	11/19/2017 20:25:22	3	SUCCESS	3	0	0	
122	11/19/2017 20:23:03	3	SUCCESS	3	0	0	
121	11/19/2017 20:20:25	3	SUCCESS	3	0	0	
120	11/19/2017 20:16:14	3	SUCCESS	3	0	0	
119	11/19/2017 20:15:10	1	SUCCESS	1	0	0	
118	11/19/2017 20:14:45	1	NO_ELIGIBLE_TASKS	0	0	1	
117	11/19/2017 19:55:17	1	NO_ELIGIBLE_TASKS	0	0	1	

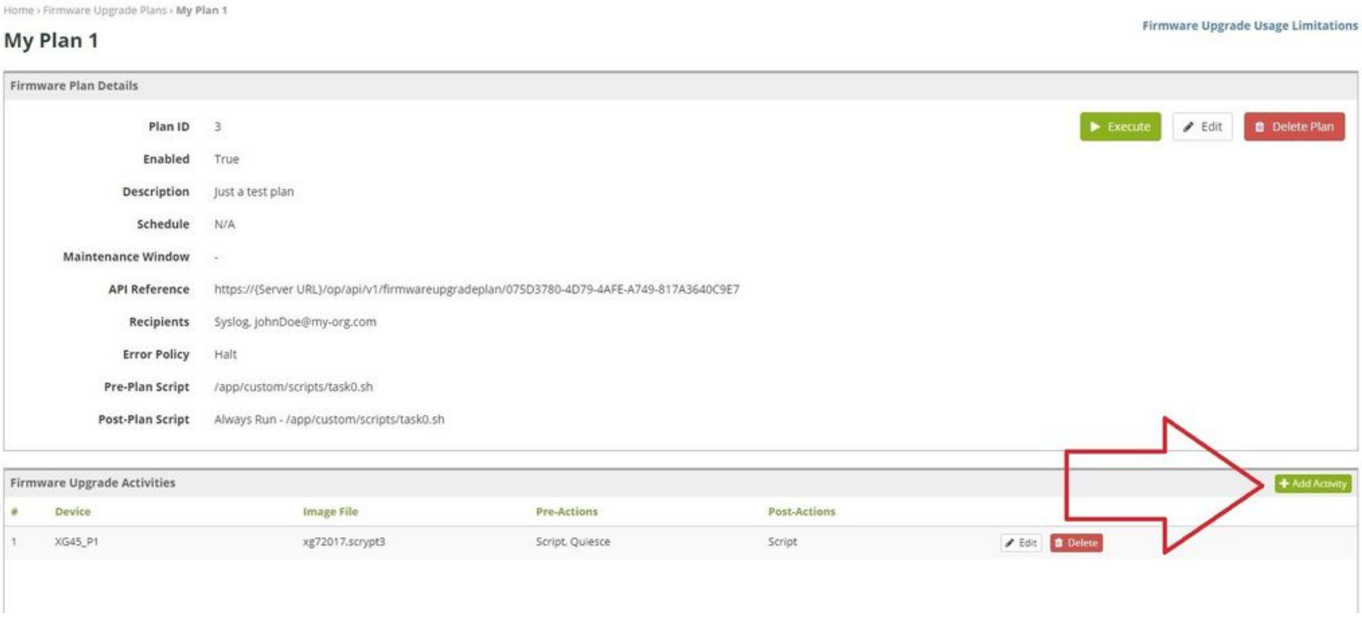
The Plan Details page is composed of three parts:

1. Plan Details - Displays the plan details, and lets the user Edit the plan, Delete it, or execute it in an ad-hoc manner (only for enabled plans)
2. Activities - Add, Edit or Delete a firmware upgrade activity
3. Recent Firmware Upgrade Plan Executions - Displays results for the most recent 40 executions of the plan - see Maintenance Plans Status Description for descriptions of the possible plan statuses

Firmware Upgrade Activity

A Firmware Upgrade Activity defines which devices should be upgraded, to which versions, the pre/post actions and the error policy to use.

To add a new firmware upgrade activity, navigate to Mange Maintenance Firmware Upgrade, select the plan to add an activity to and click "Add Activity" from the Firmware Upgrade Plan Details Page.


Home › Firmware Upgrade Plans › My Plan 1
Firmware Upgrade Usage Limitations
Execute
Edit
Delete Plan
Add Activity
Edit
Delete

My Plan 1

Firmware Plan Details

Plan ID	3
Enabled	True
Description	Just a test plan
Schedule	N/A
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/firmwareupgradeplan/075D3780-4D79-4AFE-A749-817A3640C9E7
Recipients	Syslog, johnDoe@my-org.com
Error Policy	Halt
Pre-Plan Script	/app/custom/scripts/task0.sh
Post-Plan Script	Always Run - /app/custom/scripts/task0.sh

Firmware Upgrade Activities

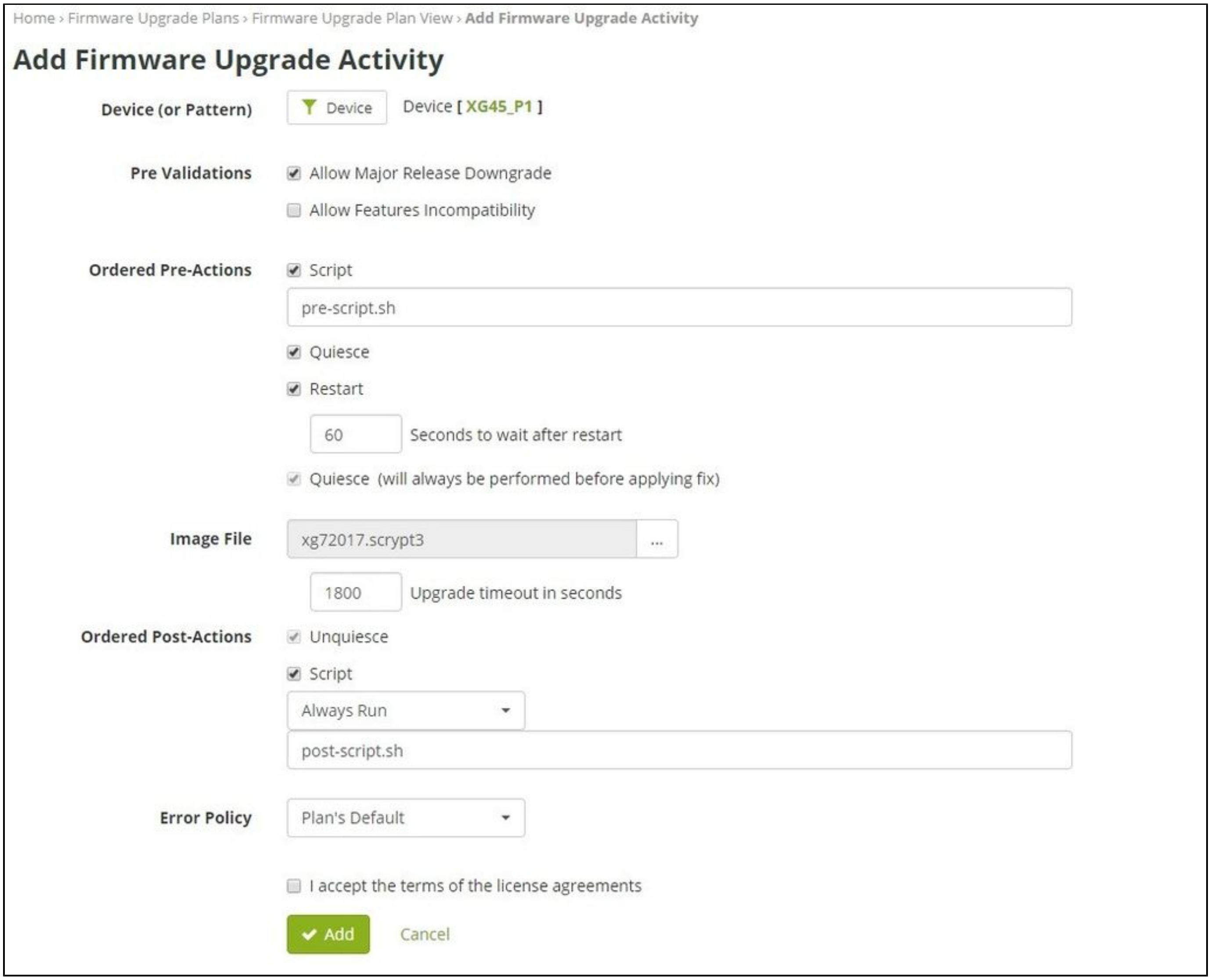
#	Device	Image File	Pre-Actions	Post-Actions
1	XG45_P1	xg72017.scrypt3	Script, Quiesce	Script

The system will display "Add Firmware Upgrade Activity" page. Consult the screenshot and the table below in order to create a new activity in the system.

Uploading Firmware Image File to DPOD

Before DPOD can use a firmware image, it needs to be uploaded into the DPOD's path that was defined in the system parameter "Firmware Upgrade - Repository Path".
You can use SCP/WinSCP or any other file transfer program to upload the file.

Add Activity Page



Home › Firmware Upgrade Plans › Firmware Upgrade Plan View › **Add Firmware Upgrade Activity**

Add Firmware Upgrade Activity

Device (or Pattern) Device Device [XG45_P1]

Pre Validations
☑ Allow Major Release Downgrade
□ Allow Features Incompatibility

Ordered Pre-Actions
☑ Script
pre-script.sh
☑ Quiesce
☑ Restart
60 Seconds to wait after restart
☑ Quiesce (will always be performed before applying fix)

Image File xg72017.scrypt3 ...
1800 Upgrade timeout in seconds

Ordered Post-Actions
☑ Unquiesce
☑ Script
Always Run
post-script.sh

Error Policy Plan's Default

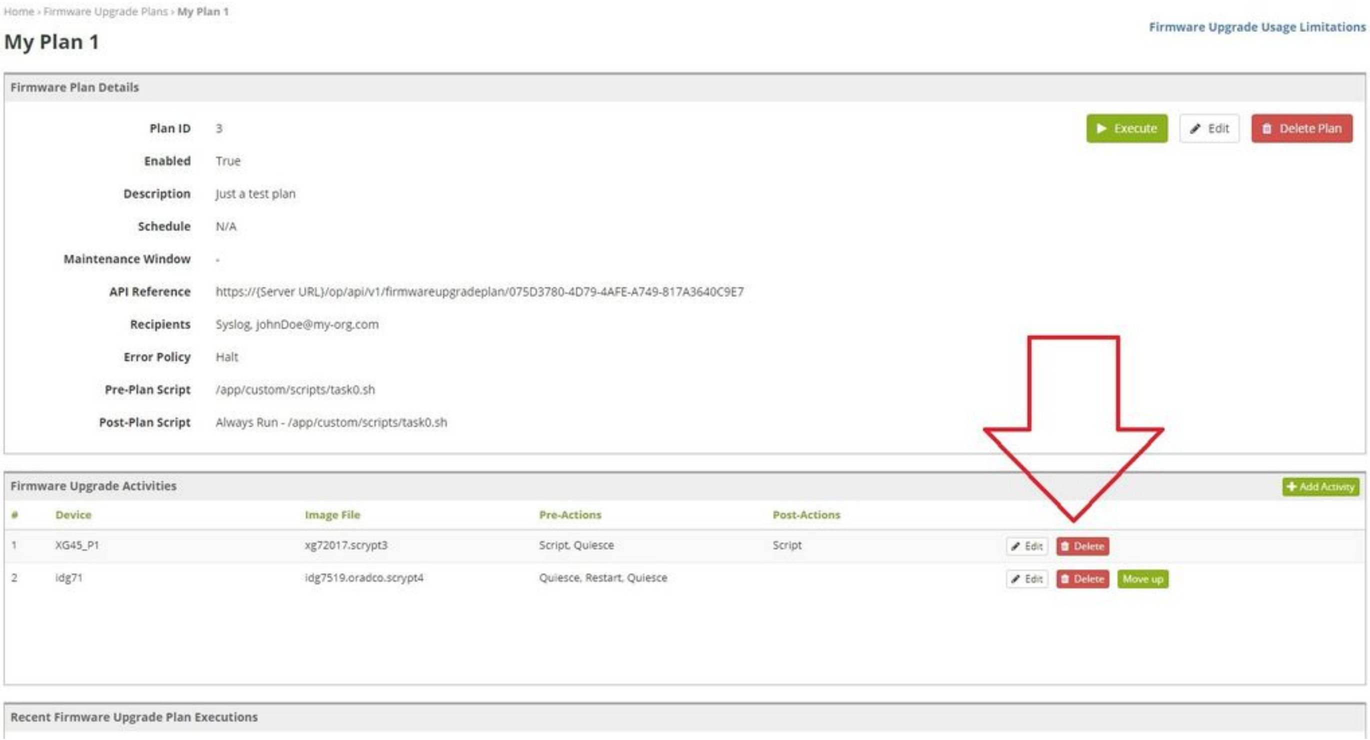
□ I accept the terms of the license agreements

Attribute	Is Mandatory?	Description
Device (or Pattern)	Yes	The Device(s) to upgrade, enter a specific device, pattern with asterisk or a list of devices or patterns See Using Patterns for Device and Domain Names in the Maintenance Concepts page
Allow Major Release Downgrade	No	Can the device be downgraded within the same major release? For example, 7.5.1.5 to 7.5.1.3 Other types of downgrade are not supported or trying to upgrade to the same firmware level are not supported.
Allow Features Incompatibility	No	Allows to upload a firmware image file that is missing features that are found on the device (Tibco-EMS and DCO-Oracle) Uploading an image that contains features that are not found in the device is not supported.
Pre-Action Script	No	A user defined script to run before the task is executed. The task will not be executed If the script fails (the return code was greater than 0) See user defined scripts for more information

Pre-Action Quiesce	No	Should the device(s) be quiesced before it is restarted. The timeout value that is passed to the quiesce SOMA is controlled by a system parameter (see maintenance configurable parametersfor more information) The device(s) will be always quiesced before the upgrade is executed, whether or not you checked this option This option only controls the quiesce that happens before the optional restart.
Pre-Action Restart	No	Should the device(s) be restarted before the upgrade starts. Restarting the device before firmware upgrade is recommended
Seconds to wait after restart	Yes (if restart requested)	How long (in seconds) to wait after restart and before issuing the quiesce request and upgrading the firmware. This parameter is used for situations where the monitored device does not enter "ready" state immediately after device restate.
Pre-Action Quiesce	Yes	Always checked, this option cannot be changed. The device will be quiesced before the upgrade starts. The timeout value that is passed to the quiesce SOMA is controlled by a system parameter (see maintenance configurable parametersfor more information)
Image File	Yes	The firmware image file, only scrypt3, scrypt4 and tar.gz types are supported Click the Three dots button to open the file selection window, the window will show all image files that were found in the Repository path (see "Firmware Upgrade - Repository Path") If a new file was just uploaded, close and re-open the window to refresh the list.
Upgrade timeout in seconds	Yes	How long to wait before DPOD will mark the upgrade execution as failed. For example, if DPOD did not receive any response from the upgraded device after 30 minutes, it will mark the execution as failed, so a syslog/email will be sent.
Post-Action Unquiesce	No	Always checked, this option cannot be changed. If the device was upgraded successfully, the upgrade process will restart the device, causing it to start unquiesced. If the upgrade failed, DPOD will automatically unquiesce the device.
Post-Action Script	No	A user defined script to run after the task is executed. The user selects whether the script should run always when a task completes, or only when the task execution fails. See user defined scripts for more information
Error Policy	Yes	Select how this activity handles errors. **Plan's Default** - Use the value that was set for the plan **Halt** - When the task failed validation or execution, stop all other tasks from this plan that are waiting for execution **Ignore** - When the task failed validation or execution, ignore and continue to run other tasks from this plan
Accept License Chechbox	Yes	Accept IBM's license is needed before firmware upgrade

Edit, Delete or Reorder Activities

The Firmware Upgrade Plan Details Page allows the user to edit, delete or reorder activities.
When the plan is scheduled to run, the activities will be processed in the order they were defined (see Firmware Upgrade Execution for more information)



Home › Firmware Upgrade Plans › My Plan 1
Firmware Upgrade Usage Limitations
Execute
Edit
Delete Plan
Add Activity

My Plan 1

Firmware Plan Details

Plan ID	3
Enabled	True
Description	Just a test plan
Schedule	N/A
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/firmwareupgradeplan/075D3780-4D79-4AFE-A749-817A3640C9E7
Recipients	Syslog, johnDoe@my-org.com
Error Policy	Halt
Pre-Plan Script	/app/custom/scripts/task0.sh
Post-Plan Script	Always Run - /app/custom/scripts/task0.sh

Firmware Upgrade Activities

#	Device	Image File	Pre-Actions	Post-Actions	
1	XG45_P1	xg72017.scrypt3	Script, Quiesce	Script	Edit Delete
2	idg71	idg7519.oradco.scrypt4	Quiesce, Restart, Quiesce		Edit Delete Move up

Recent Firmware Upgrade Plan Executions

Firmware Upgrade Execution (Tasks)

This page describes how DPOD prepares the execution flow of a firmware upgrade plan (using tasks) and subsequently - how the tasks themselves are executed.

Task Creation Flow

General execution flow for a firmware upgrade plan:

1. Verify that the system allows Firmware Upgrades to run. (See Configurable Parameters and Settings to learn how to enable or disable all firmware upgrade activities)
2. Verify that the current system time is within the maintenance window timeframe defined for the plan
3. Verify that the image repository path that was set in system parameters actually exist (See Configurable Parameters and Settings)
4. Iterate over all the activities defined for the plan, and split them into executable tasks.
For example: consider a plan with two activities, one to upgrade devices QA* and a second to upgrade device - TEST9.
DPOD will create three tasks:
a. Firmware upgrade task for device QA1
b. Firmware upgrade task for device QA2
c. Firmware upgrade task for device TEST9
If all the created tasks are in "Skipped" state (because the devices are not available, or because no devices matched the input patterns) - the plan will stop
5. If there are any tasks waiting to be executed - the Pre-Plan Script will be executed (if requested in the plan settings)
.the plan will stop if the script's return code is higher than 0

Task Execution Flow

> Only 2 firmware upgrade tasks will be executed in parallel

After the firmware upgrade tasks are created, they will start to execute. The following is the general execution flow for a task:

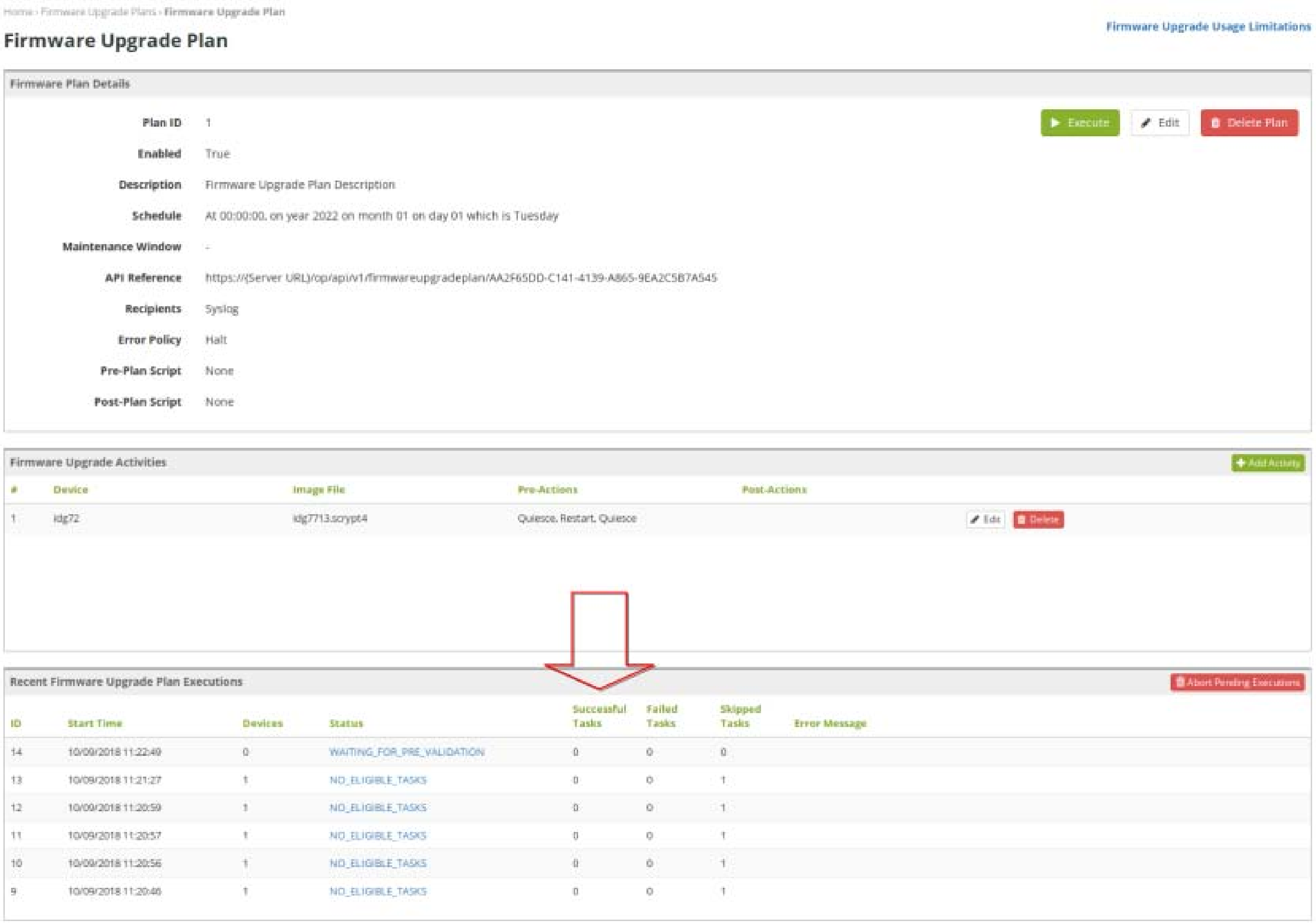
> Firmware upgrade tasks will start to execute in the order they were created, which corresponds to the order which the activities were defined.

1. Check that the image file's model type (IDG, XG, XI, XB) matches the device
2. Verify that the image file is actually an upgrade, if it's a downgrade, DPOD will only allow downgrade to the same major release (if the user checked the "Allow Major Release Downgrade" option in the activity)
3. Check that the same features appear in the image and device (Tibco-EMS and/or Dco-Oracle)
If features present in the image but not in the device - stop
If the features present in the device but not in the image - stop - unless the user checked the "Allow Features Incompatibility" option in the activity.
4. Check that the image file's format matches the device (scrypt3 for physical devices or scrpyt4 for virtual devices)
5. Verify that there is enough space in the encrypted and temporary file systems to upload the selected image file
6. Check that there are no unsaved changes in any domains in the device
7. Check that there are no quiesced domains in the device
8. Run the user's pre-script (if requested in the activity), the task will stop if the script return value is larger than 0
9. Issue a Quiesce domain/device SOMA (if requested for the activity)
10. Wait for the device or domain to finish quiescing. A timeout value may be specified for the Quiesce SOMA (see Configurable Parameters and Settings),
DPOD will cancel the task if the domain(s) are not yet quiesced 3 minutes after the specified timeout, and will issue an Unquiesce SOMA
11. Restart the device (if requested for the activity)
12. After the device finished restarting, wait for the time that was defined in the activity's "Seconds to wait after restart" field
13. DPOD will upload the firmware image to the monitored device
14. Issue a Quiesce domain/device SOMA - this step will always run, even if the user did not ask for a quiesce before the restart
15. Once all the domains are quiesced - start the firmware upgrade
16. Wait for the upgrade to finish,
The maximum time that DPOD will wait for the upgrade to finish is defined in the activity's "Upgrade timeout in seconds" field,
17. Run the user's post-task script (if requested in the activity)

When all the plan's tasks completed execution, the post-plan script will be executed (if requested in the plan settings)

Firmware Upgrade Execution Results

The Plan Details page shows the 40 most recent plan execution results,



Home › Firmware Upgrade Plans › Firmware Upgrade Plan
Firmware Upgrade Usage Limitations
Execute
Edit
Delete Plan
Add Activity
Edit
Delete
Abort Pending Executions

Firmware Upgrade Plan

Firmware Plan Details

Plan ID	1
Enabled	True
Description	Firmware Upgrade Plan Description
Schedule	At 00:00:00, on year 2022 on month 01 on day 01 which is Tuesday
Maintenance Window	-
API Reference	https://{Server URL}/op/api/v1/firmwareupgradeplan/AA2F65DD-C141-4139-A865-9EA2C5B7A545
Recipients	Syslog
Error Policy	Halt
Pre-Plan Script	None
Post-Plan Script	None

Firmware Upgrade Activities

#	Device	Image File	Pre-Actions	Post-Actions
1	idg72	idg7713.scrypt4	Quiesce, Restart, Quiesce	

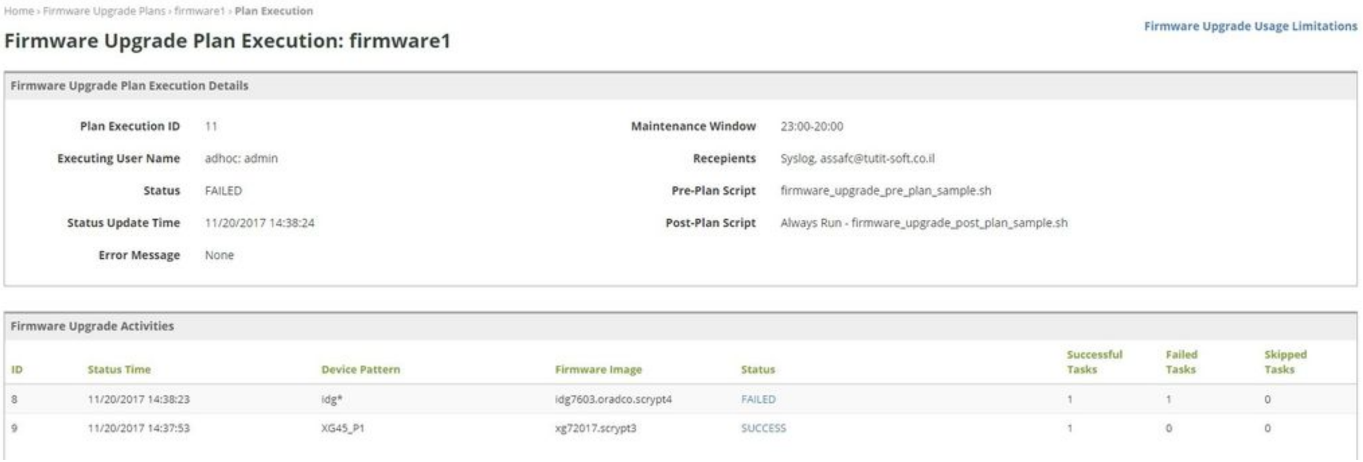
Recent Firmware Upgrade Plan Executions

ID	Start Time	Devices	Status	Successful Tasks	Failed Tasks	Skipped Tasks	Error Message
14	10/09/2018 11:22:49	0	WAITING_FOR_PRE_VALIDATION	0	0	0	
13	10/09/2018 11:21:27	1	NO_ELIGIBLE_TASKS	0	0	1	
12	10/09/2018 11:20:59	1	NO_ELIGIBLE_TASKS	0	0	1	
11	10/09/2018 11:20:57	1	NO_ELIGIBLE_TASKS	0	0	1	
10	10/09/2018 11:20:56	1	NO_ELIGIBLE_TASKS	0	0	1	
9	10/09/2018 11:20:46	1	NO_ELIGIBLE_TASKS	0	0	1	

The table outlines the following details for each plan execution

Column Name	Description
ID	The Plan Execution ID
Start Time	The time the plan entered the execution queue
Devices	Number of devices that were supposed to be upgraded. Both failed and successful upgrades are aggregated.
Status	The current status of the plan
Successful Tasks	Number of upgrade tasks that completed successfully for this plan execution
Failed Tasks	Number of upgrade tasks that failed for this plan execution
Skipped Tasks	Number of upgrade tasks that did not execute, e.g. because the device was not available
Error Message	Plan's Error message (If any)

*Click the red "Abort Pending Executions" to stop execution in status "WAITING_FOR_PRE_VALIDATION" that did not started yet.
**Click the status column to drill into the activities execution details page.



Home › Firmware Upgrade Plans › firmware1 › Plan Execution

Firmware Upgrade Plan Execution: firmware1

Firmware Upgrade Usage Limitations

Firmware Upgrade Plan Execution Details

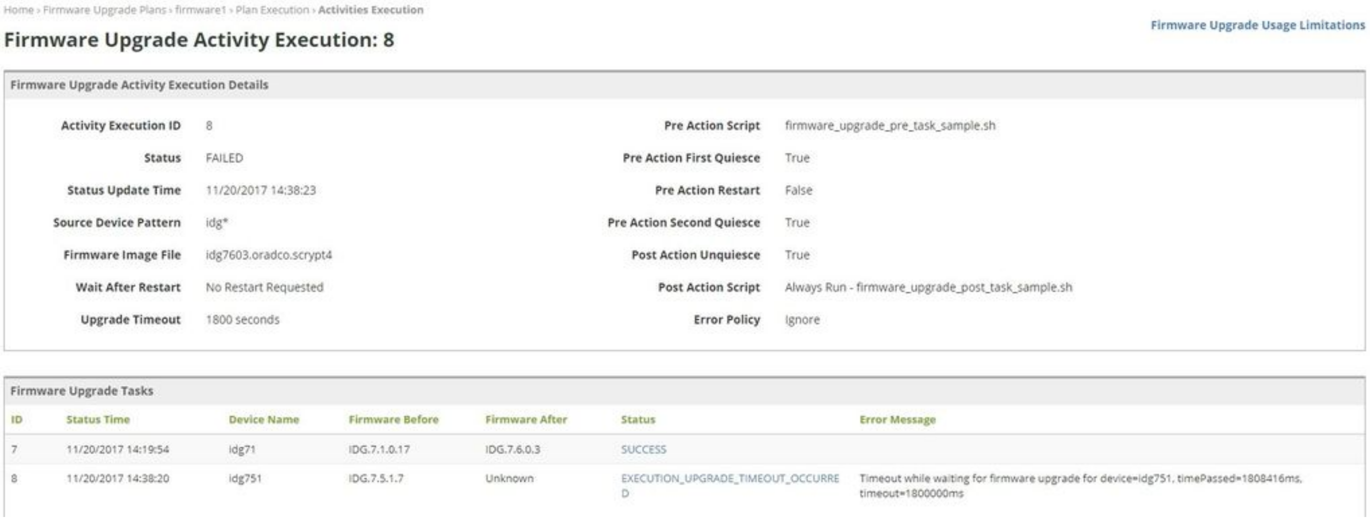
Plan Execution ID	11	Maintenance Window	23:00-20:00
Executing User Name	adhoc: admin	Recepients	Syslog, assafc@tutit-soft.co.il
Status	FAILED	Pre-Plan Script	firmware_upgrade_pre_plan_sample.sh
Status Update Time	11/20/2017 14:38:24	Post-Plan Script	Always Run - firmware_upgrade_post_plan_sample.sh
Error Message	None		

Firmware Upgrade Activities

ID	Status Time	Device Pattern	Firmware Image	Status	Successful Tasks	Failed Tasks	Skipped Tasks
8	11/20/2017 14:38:23	idg*	idg7603.oradco.scrypt4	FAILED	1	1	0
9	11/20/2017 14:37:53	XG45_P1	xg72017.scrypt3	SUCCESS	1	0	0

Column Name	Description
ID	The Activity Execution ID
Status Time	The last time the status of the activity changed
Device Pattern	The device name or pattern that was used for this firmware upgrade activity
Firmware Image	The name of the image file selected for the upgrade
Status	The current status of the activity
Successful Tasks	Number of upgrade tasks that completed successfully for this activity execution
Failed Tasks	Number of upgrade tasks that failed for this activity execution
Skipped Tasks	Number of upgrade tasks that were skipped for this activity execution

Click the status column to drill into the task execution details page



Home › Firmware Upgrade Plans › firmware1 › Plan Execution › Activities Execution

Firmware Upgrade Activity Execution: 8

Firmware Upgrade Usage Limitations

Firmware Upgrade Activity Execution Details

Activity Execution ID	8	Pre Action Script	firmware_upgrade_pre_task_sample.sh
Status	FAILED	Pre Action First Quiesce	True
Status Update Time	11/20/2017 14:38:23	Pre Action Restart	False
Source Device Pattern	idg*	Pre Action Second Quiesce	True
Firmware Image File	idg7603.oradco.scrypt4	Post Action Unquiesce	True
Wait After Restart	No Restart Requested	Post Action Script	Always Run - firmware_upgrade_post_task_sample.sh
Upgrade Timeout	1800 seconds	Error Policy	Ignore

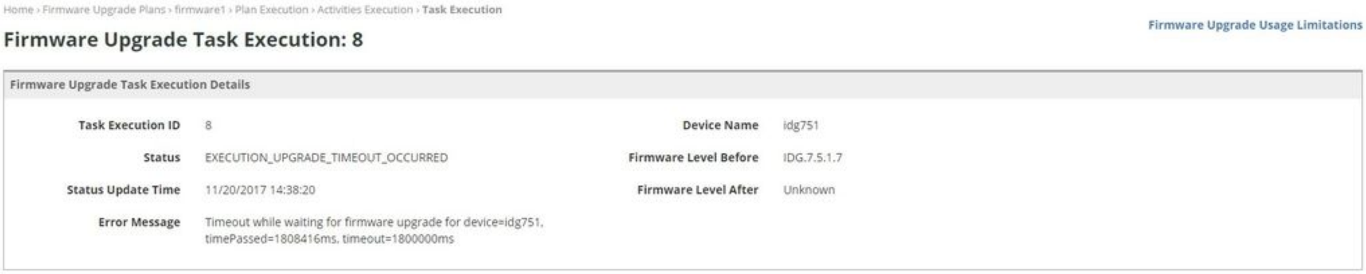
Firmware Upgrade Tasks

ID	Status Time	Device Name	Firmware Before	Firmware After	Status	Error Message
7	11/20/2017 14:19:54	idg71	IDG.7.1.0.17	IDG.7.6.0.3	SUCCESS	
8	11/20/2017 14:38:20	idg751	IDG.7.5.1.7	Unknown	EXECUTION_UPGRADE_TIMEOUT_OCCURRED	Timeout while waiting for firmware upgrade for device=idg751, timePassed=1808416ms, timeout=1800000ms

Column Name	Description
ID	The Task Execution ID
Status Time	The last time the status of the task changed
Device Name	The Device being upgraded

Firmware Before	The firmware level of the device before the task run
Firmware After	The firmware level of the device after the task run or "Unchanged" if the device was not upgraded. During the run, the column may show "Unchanged" if a timeout occured while waiting the upgrade to complete, the column will show 'Unknown"
Status	The current status of the task
Error Message	Task's Error message if any

Click the status column to drill into the downloaded files details page


Home › Firmware Upgrade Plans › firmware1 › Plan Execution › Activities Execution › Task Execution
Firmware Upgrade Usage Limitations

Firmware Upgrade Task Execution: 8

Firmware Upgrade Task Execution Details

Task Execution ID	8	Device Name	idg751
Status	EXECUTION_UPGRADE_TIMEOUT_OCCURRED	Firmware Level Before	IDG.7.5.1.7
Status Update Time	11/20/2017 14:38:20	Firmware Level After	Unknown
Error Message	Timeout while waiting for firmware upgrade for device=idg751, timePassed=1808416ms, timeout=1800000ms		

Firmware Upgrade - User Defined Scripts

DPOD allows execution of user defined, custom scripts before and after both Plan and Task execution.
The scripts are executed from /app/custom/scripts (See Configurable Parameters and Settings for information on how to change this path)

> Any script that returns a return code larger than 0 is considered to have failed.
>
> if a pre-plan or a pre-task script failed - the plan or task will be flagged as failed and will **not** execute.
> If a pre-task script failed, the post-task script will still be executed (if requested)

DPOD will send certain parameters to the script, to indicate the execution details and completion status.

Parameters Sent to the Firmware Upgrade Pre-Plan Script

Sample script: /app/custom/scripts/firmware_upgrade_pre_plan_sample.sh

1=PLAN_TYPE - The constant "FIRMWARE-UPGRADE-PLAN"
2=PLAN_STAGE - The constant "PRE"
3=PLAN_ID - The ID of the firmware upgrade plan
3=PLAN_NAME - The name of the firmware upgrade plan

Example:
1=FIRMWARE-UPGRADE-PLAN
2=PRE
3=16
4=firmware1

Parameters Sent to the Firmware Upgrade Post-Plan Script

Sample script: /app/custom/scripts/firmware_upgrade_post_plan_sample.sh

1=PLAN_TYPE - The constant "FIRMWARE-UPGRADE-PLAN"
2=PLAN_STAGE - The constant "POST"
3=PLAN_ID - The ID of the firmware upgrade plan
4=PLAN_NAME - The name of the firmware upgrade plan
5=FINAL_STATUS_CODE - Final status code of the firmware upgrade plan
6=FINAL_ERROR_MSG - Final error message of the firmware upgrade plan, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=TASKS_VALUES - list of comma separated values for each task - task ID, device name, version before execution, version after execution, task status - different tasks are separated with ~ (Tilde sign)

Example:
1=FIRMWARE-UPGRADE-PLAN
2=POST
3=16
4=firmware1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=13,IDG-QA-2,IDG.7.5.0.17,IDG.7.5.2.10,SUCCESS~14,IDG-QA-3,IDG.7.5.0.17,IDG.7.5.2.10,SUCCESS

Parameters Sent to the Firmware Upgrade Pre-Task Script

Sample script: /app/custom/scripts/firmware_upgrade_pre_task_sample.sh

1=TASK_TYPE - The constant "FIRMWARE-UPGRADE-TASK"
2=TASK_STAGE - The constant "PRE"
3=TASK_ID - The ID of the firmware upgrade task
4=PLAN_NAME - The name of the firmware upgrade plan that generated this task
5=DEVICE_NAME - The name of the device
6=DEVICE_HOST - The host of the device
7=SOMA_PORT - The soma port of the device
8=VERSION_BEFORE - The firmware version of the device before the task started
9=IMAGE_FILE_NAME - the image file name to use for the upgrade

Example:
1=FIRMWARE-UPGRADE-TASK
2=PRE

3=12
4=firmware1
5=IDG-QA-2
6=192.168.72.100
7=5550
8=IDG.7.5.0.17
9=idg75210.oradco.scrypt4

Parameters Sent to the Firmware Upgrade Post-Task Script

Sample script: /app/custom/scripts/firmware_upgrade_post_task_sample.sh

1=TASK_TYPE - The constant "FIRMWARE-UPGRADE-TASK"
2=TASK_STAGE - The constant "POST"
3=TASK_ID - The ID of the firmware upgrade task
4=PLAN_NAME - The name of the firmware upgrade plan that generated this task
5=FINAL_STATUS - Final status code of the firmware upgrade task
6=FINAL_ERROR_MSG - Final error message of the firmware upgrade task, or "NONE" if there were no errors
7=FFU1 - The constant "FFU" (For future use)
8=FFU2 - The constant "FFU" (For future use)
9=DEVICE_NAME - The name of the device
10=DEVICE_HOST - The host of the device
11=SOMA_PORT - The soma port of the device
12=VERSION_BEFORE - The firmware version string before the task was started
13=VERSION_AFTER- The firmware version string after the task finished
14=IMAGE_FILE_NAME - the image file name to use for the upgrade

Example:
1=FIRMWARE-UPGRADE-TASK
2=POST
3=13
4=firmware1
5=SUCCESS
6=NONE
7=FFU
8=FFU
9=IDG-QA-2
10=192.168.72.100
11=5550
12=IDG.7.5.0.17
13=IDG.7.5.2.10
14=idg75210.oradco.scrypt4

Publish Firmware Upgrade Events via Syslog and Email

Setup

1. The maintenance configurable parameters page provides information on how to setup the syslog destination.
2. The Email destination is configured in the plan definition.
3. Configure the SMTP parameters from the System Parameters Page, see the System Parameters List Page for a description of each parameter.
4. If you set a value for "The HTTP Address of the UI" parameter - a link to the DPOD UI will be added to the emails with a shortcut to the relevant plan or task execution results.

The following events will be published via Email and/or syslog (as defined in the firmware upgrade plan):

Plan Events

Firmware Upgrade Plan Completed Successfully
All upgrade tasks finished successfully
Syslog Message Id - 0x00a0450a

Firmware Upgrade Plan Completed Successfully with Skipped Tasks
Some upgrade tasks finished successfully and some were skipped (but none failed)
Syslog Message Id - 0x00a0451a

Firmware Upgrade Plan Failed
At least one task failed
Syslog Message Id - 0x00a0452a

Task Events

Firmware Upgrade Task Completed Successfully
A firmware upgrade task finished execution, and all files downloaded to the user's storage
Syslog Message ID - 0x00a0250a

Firmware Upgrade Task Failed
A firmware upgrade task failed for any reason
Syslog Message ID - 0x00a0251a

Firmware Upgrade Task Skipped
When a firmware upgrade task did not execute - e.g. when the device was unavailable
Syslog Message ID - 0x00a0253a

Firmware Upgrade Task Long Running
If a task's status did not change for more than 60 minutes (see maintenance configurable parameters for more information), DPOD will issue the "Long Running" event and will consider the task as finished
Syslog Message ID - 0x00a0254a

Firmware Upgrade Task was not Executed
For tasks that passed all validations but did not execute. E.g. when the maintenance window timeframe ended before the task was executed
Syslog Message ID - 0x00a0255a

Appliance Migration

OVERVIEW

The Appliance Migration wizard helps with migration of a source gateway to a different target gateway,
It automatically performs secure-backup on the source gateway, and secure-restore on the target gateway, while providing an easy step-by-step wizard to guide the admin in the process.

APPLIANCE MIGRATION STEPS:

1. Limitations and prerequisites
2. input the source and target gateways details
3. Pre-Backup Validations
4. Secure-Backup of the source gateway
5. Removal of the source gateway from DPOD (optional)
6. Pre-restore validations
7. Secure-Restore to the target gateway

Appliance Migration Limitations and Prerequisites

List of Supported Gateways

- Source Gateways - XG45, XI52, XB52, IDG, IDG X2
- Target Gateways - IDG, IDG X2
- Physical & Virtual (OVA) Form Factor only

Prerequisites & Assumptions

- The source and the target gateways should be up and running to perform backup and restore (not necessarily at the same time).
- The source gateway must be registered to DPOD before process begins.
- Target gateway may or may not be registered to DPOD before the process begins.
- Target gateway must have XML Management Interface enabled. The XML Management Interface must be accessible via the MGMT network interface.
- The system must be able to communicate with the XML Management Interface of both gateways using SOMA requests with supplied user and password.
- Target gateway will have a temporary management IP address (before the restore) to allow running the Secure-Restore.
- Target gateway will have a different system identifier (device name) than the source gateway.
- Private and public keys must be available before secure backup or restore start.
- Public key must be uploaded to the source gateway while Crypto IC object must be uploaded to the target gateway before the restore begins.

API Connect

If the source gateway is part of an API-Connect environment, please pay attention to the following notes:

- When connecting a gateway to an API Connect environment for the first time, the Application Optimization feature is automatically enabled on that gateway.
- To complete the restore phase of this migration process, the target gateway must also have the Application Optimization feature enabled.
- If the Application Optimization feature is not enabled on the target gateway, you may contact the gateway support team for assistance.

Limitations

- The migration process cannot be executed in DPOD's Developer or Docker Edition.
- The migration process will **not** handle the following:
  - B2B persistence store data
  - HSM data
  - RAID data
  - Gateways configured with Application Optimization
  - Gateways configured with Link Aggregation/Standby-Control
  - Custom system health metrics, device groups and DNS translations configured for the source gateway in the system

Next: Input basic details

Appliance Migration - Step 1 - Input Basic Details

The "Basic Details" page contains input fields for the source and target gateways details.

Source Gateway

The source gateway needs to be an existing gateway, which was already configured to DPOD (via the ManageDevicesGateway)
Admin Password (Only appears if the DPOD uses a gateway user which is not "admin") - see "Changing the Admin Password" later on this page
Source Gateway - the name of the source gateway.
Certificate Name - the certificate that will be used for the Secure-Backup process

> The Secure-Restore step will require you to create a Crypto Identification Credentials object on the target gateway.
> The Certificate you provide on the basic details step and the Crypto Key will be required for you to create this object.
> **Do not start the process** unless you have **both** of them available and at reach.

Quiesce - Whether a quiesce should be performed before the Secure-Backup starts.

Target Gateway

> The target gateway details are the details of the gateway **before** the Secure-Restore, **and not** the future post-restore details.

Target Gateway - If the target gateway is configured to DPOD, choose "Existing Monitored Gateway", and choose the gateway name from the device filter.
If the target gateway was not configured in DPOD choose "New gateway" and enter the gateway details:

- Name - the gateway name ("Appliance Name" in the gateway's system settings)
- SOMA Address and Port - address and port of the gateway's XML Management Interface
- SOMA User and password - the user and password that will be used to issue commands to the gateway

Crypto IC - the name of the Crypto Identification Credentials object, you will need to create this object on the target gateway **before** the Secure-Restore starts.
Quiesce - Whether a quiesce should be performed before the Secure-Restore starts..

Changing the Admin Password

After Secure-Restore is run on the target gateway, the admin user's password will always be changed to "admin"
If DPOD is already using the admin user for the source gateway, the migration process will automatically change the admin password on the target gateway to the source gateway's admin password.
If DPOD is using a different user, the migration process will change the admin password to the password you entered in the "Admin Password" field of the Source Gateway details.

Next: Pre-Backup validations

Appliance Migration - Step 2 - Pre-Backup Validations

Overview

The pre-backup validations step will perform two types of checks:

1. Checks on the source gateway that is about to be backed-up
2. Compatibility checks on the target gateway - only if the target gateway is available at this stage

> It is not mandatory, **but highly recommended** to have the target gateway up and running at this stage, so DPOD can check that the hardware, firmware and features are compatible between the source and target gateways.
>
> If the target gateway is not available at this stage - DPOD will run those checks later on, just before the Secure-Restore.

Validations

1. Application edition - checks that DPOD is not running on Docker or Developer Edition.
2. Secure Backup mount point - the path where DPOD will download the backup to (and upload the backup from) should be a dedicated mounted filesystem - the mount point is set in the System Parameters page (under "Backups - Destination Path")
3. Source is in Secure Backup mode - checks whether the source gateway's Backup Mode is "Secure backup", if the gateway is in "Normal" mode - no Secure Backups or Secure Restores can be issued against it.

If the target gateway is available, more validations will be done at this stage:

4. Target is in Secure Backup mode - checks whether the target gateway's Backup Mode is "Secure backup", if the gateway is in "Normal" mode - no Secure Backups or Secure Restores can be issued against it.
5. Identical firmware level - the source and target gateways must be on the same firmware level, if you need to upgrade the target gateway, consider using DPOD's Firmware Upgrade feature
6. Gateway features compatibility - checks whether the source and target have the same license and features (such as ORA-DCO) - this is an informational check, the user can choose to mark it as "ignored" if it fails.
7. Hardware compatibility - checks whether the gateways' device types are compatible (for example, an IDG gateway cannot be migrated to XG45) - this is an informational check, the user can choose to mark it as "ignored" if it fails.

Next: Source Secure-Backup

Appliance Migration - Step 3 - Source Secure Backup

A Secure-Backup command will be issued at this point.

> The gateway's Secure-Backup will be done using an ad-hoc DPOD Backup plan.
> Please review the backup limitations and notes on this page

Before the backup command is issued, you may change the Certificate Name selection, and whether the gateway will be quiesced or not.

Once started, the status of the backup will be displayed on the lower part of the page,
If you wish to view more details about the backup process - click the status to go to DPOD's Backup Plan Execution page

You can either stay on the wizard and wait (the status will be refreshed automatically), or exit the wizard and come back anytime.
The wizard will advance automatically once the backup is completed successfully.

If the backup failed for any reason, and error message will be displayed, consult Backup Tasks Status Codes for a complete list of backup statuses, fix the issue and click "next" again to re-run the backup process.

Next: Source Removal

Appliance Migration - Step 4 - Source Removal

The source removal step will keep or remove the gateway from DPOD.

> This step **does not** perform any actions on the source gateway itself, it is your responsibility to disconnect or to change the gateway's configuration

Choose "Remove Source Gateway" - to remove the source gateway from DPOD.
Even after the gateway is removed from DPOD, you will still be able to see old transactions and syslog data from this gateway in DPOD (depends on your storage capacity)

Choose "Keep Source Gateway" to keep the source gateway in DPOD after the migration is done.
The Secure-Restore process will assign the same source IP address to the target gateway - so if you wish to keep both - you will need to manually change the source's IP address and enter it in the input fields "New Source Gateway SOMA Address","New Source Gateway SOMA Port" and "New Source Gateway Log Target Source Address".

Next: Pre-restore validations

Appliance Migration - Step 5 - Pre-Restore Validations

Overview

At this point, the target gateway needs to be up and running, DPOD will perform compatibility checks to make sure the source and target gateways are compatible.
Some of the validations were already performed during Step 2 - Pre-Backup Validations, if the target gateway was available at this stage.

Validations

1. Target is in Secure Backup mode - checks whether the target gateway's Backup Mode is "Secure backup", if the gateway is in "Normal" mode - no Secure Backups or Secure Restores can be issued against it.
2. Identical firmware level - the source and target gateways must be on the same firmware level, if you need to upgrade the target gateway, consider using DPOD's Firmware Upgrade feature
3. Gateway features compatibility - checks whether the source and target have the same license and features (such as ORA-DCO) - this is an informational check,the user can choose to mark it as "ignored" if it fails.
4. Hardware compatibility - checks whether the gateways device type is compatible (for example, and IDG gateway cannot be migrated to XG45) - this is an informational check, the user can choose to mark it as "ignored" if it fails.
5. Target appliance name matches user input - checks that the target name that was entered in the "Basic Details" step matches the actual target appliance name.
   If it is not - either change the appliance name, or edit the details that were entered for the target gateway (There are input fields to edit the target gateway details, just below the list of validations)
6. Network Interfaces - DPOD will check that only the Management Network Interfaces are up - this is an informational check, the user can choose to mark it as "ignored" if it fails.
   If there are no "mgt" or "mgmt" interfaces, DPOD will be unable to do the validation and it will be marked as failed - the user will then need to manually check and mark this validation as "ignored".

Next: Secure Restore

Appliance Migration - Step 6 - Target Secure Restore

A Secure-Restore command will be issued at this point.

Before the Secure-Restore command is issued, you can change the Crypto Identification Credentials object name and choose whether the target gateway will be quiesced before the restore starts.

Once started, the status of the restore will be displayed on the lower-right part of the page,
You can either stay on the wizard and wait (the status will be refreshed automatically), or exit the wizard and come back anytime.
The wizard will advance automatically once the backup is completed successfully.

> While the restore is running, please do not try to login to the target gateway and/or change the admin password.

The Restore process will execute the following steps:

1. Pre-checks - whether the backup files are found on the filesystem, whether the target gateway's encrypted filesystem has enough space for uploading the backup and whether the Crypto Identification Credential object exists and up.
2. Upload Backup files to the target's encrypted filesystem.
3. Run Secure-Restore with validation=on, the process will stop if any errors are returned.
4. Quiesce (optional)
5. Run Secure-Restore with validation=off - actually runs the secure-restore, **all existing gateway's data will be erased**
6. Wait for the Secure-Restore and for the following restart to complete
7. Post Setup:
    - Change the admin password to the source's admin password (or, if DPOD is not using the admin user, to the password that was entered on Step 1 - Input Basic Details
    - Change the target appliance name to the name entered on Step 1 - Input Basic Details
    - Setup the gateway to work with DPOD - all previous setup will be copied (Syslog agent's selection for each domain, analysis levels and WS-M setup)

Next: Manual Configuration

Appliance Migration - Step 7 - Manual Configuration

The "Manual Configuration" page outlines manual setup you may need to perform after the secure restore to the target gateway was done:

- Non-mgmt network interfaces should be still disconnected at the target gateway.
  To enable applicative traffic on the target gateway, please configure the source gateway's and/or target gateway's network interfaces in a way that will not cause IP address collisions.
- If the source gateway was part of an API-Connect gateway cluster, you might need to make API-Connect aware of the migration by removing the gateway from the cluster and adding it back again.

Security

This section contains information about the security and access control implementation throughout DPOD.

The section is divided into the following topics:

- Web Console Security
- Product Components
- Virtual Appliance Security
- Firewall Requirements
- External Self Service Console
- Operating System Users

Web Console Security

DPOD's Web Console enables the user to view all the information gathered, processed and analyzed by DPOD.

This useful information can be highly confidential. DPOD therefore implements a suite of security functions in order to enable confidentiality and Role Based Access Control to DPOD's functions and information.

SECURE WEB ACCESS

DPOD has the following features securing web access:

- Access to DPOD's Web Console is provided via a supported web browser over HTTPS (SSL).
- The Console uses a self-signed certificate and a key (in PEM format) generated during DPOD's installation process. The user should replace them with the organization’s certificate.
- Audit log (access log) exists and is enabled by default. The user may configure its format in /app/ui/MonTier-UI/conf/server.xml (under the key "access_log").
- Session timeout is set to 30 minutes by default. The user may change this default in /app/ui/MonTier-UI/conf/web.xml (under the key "session-timeout").
- DOD Lockout is enabled by default. The user may configure the number of retries and period of lockout in /app/ui/MonTier-UI/conf/server.xml (change LockOutRealm parameters as required).
  For example: <Realm className="org.apache.catalina.realm.LockOutRealm" **failureCount="3" lockOutTime="300" cacheSize="1000" cacheRemovalWarningTime="3600"**>
- Admin users access may be limited by IP address. See Limit Admin Users Access by IP.

Certificate Replacement

The process described in this page will let an administrator replace the default DPOD's web console certificate with one signed by the organization.

Before You Begin

You will need:

- Access to the DPOD's appliance
- The new certificate and key files

Process

1. Log in to DPOD's appliance.
2. Copy the new certificate and key file either to the current certificate directory on the DPOD appliance or to any other directory of your choice.
   The current certificate directory is:

   ```
   /etc/httpd/conf/certs
   ```

3. Open the web server configuration file for editing:

   ```
   vi /etc/httpd/conf/httpd.conf
   ```

4. Update the SSL Certificate lines:

   ```
   SSLCertificateFile "the new certificate file path"
   SSLCertificateKeyFile "the new key file path"
   ```

   SSLCertificateKeyFile needs to point to a key of a "PEM" format.

   SSLCertificateFile needs to point to a certificate of a "DER" format.

   > The certificate / key can not be stored in a keystore (JKS, PKCS)

5. Restart the web server

   ```
   service httpd restart
   ```

6. Trouble Shooting

   a. Run syntax check on httpd configuration file to make sure certificate and key file path are valid

      ```
      apachectl -t
      ```

Valid output should be : "Syntax OK"

Wrong certificate path : "SSLCertificateFile: file '/etc/httpd/conf/certs/DPOD.cer' does not exist or is empty"

b. Make sure certificate and key file format are valid

Check key file format

```
openssl rsa -in DPOD.key -check
Valid output :
RSA key ok writing RSA key -----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA6ti29asWLikNHmici/2SjgkQWjfrzw6n2l2AQ2AxzVPGwno
y
POHWTz5+0H+WYfy0NgRNEn1KvcBqJtk26cM4NUhgdi7qP5g11u/1nkGqdJiPK3D
x
BdivYLnJEQF6gvK57nzUHkEHMLc93zTJql+O5dUgjKdkG/DnIIPl9gXUuW33lo5
V
jftvMtdSoFIJ4SVMtriSTmE8CGH49CqVu03Qp5jhfAmz83V07QcD6YpBe9MD/fd
E
hwY/Y+kH+A1mBchAGTDLLz7O8a2FYoMHgkycDuiZuIBiSzSaV6Tf/my8n4F8c+k
q
c2fFTqHZmW0H8dMRi2RNRgvQ6Kn8joN7Tev4xQIDAQABAoIBAQDoitrv/A8keiW
x
XKjWvanm1vbIPuNSzhJLWZZuIMxvomsHm3QvcPiC00FDN3MzZ8UST8P5cPMXXXY
/
LYsAgfwgVqCdperyOcfmIwm1QRSGC6KIw3cF8QAH6S89lZc4Hx0ZF6X6py11gZz
U
bjLab3DSB+4JGJ86Q5q5SaHlsPRo/qMWK934XvWpq/DejXFgEbVvGdUczafj7i8
b
5gwKeVjJnEiXYH7IeayOJv1o9awlWRy0c/eAZ6nosAfQU3QFnpGKwNRlwbC2S6z
2
HAaIF9wZt3qaTQV9gw4SwkO5RJTgCAMsC1EFgzby8dCsoK4pHjTeTTHhoHNCNs2
6
izolmLYBAoGBAPs5b+i4vfX8VGaFnaCgDJtS4/xnakHrwJtwGFS4EeMdBh/pDms
P
3rU4W6safuN3YGayt05Luu+5y1iZnioWv7ZsYFKcih5paFcVPf8ysUfdL7tAtfC
e
DZLxVpTZwct4UJ5ZPsmTBDzQDWv4OGAuyE+noCk4kXrkq1kDOTG6DHFBAoGBAO9
P
k4JQ4JpGzCk7gl3S604P7Oaq34KRP7+sJZmW2Ll/GOfLKxqmqX+yUej0lm+rsso
u
QJHND7PdC3ctKGPsPvT8nDZeFqW5LXGEC2kqYZUvIMi/isIsfdN8TR21MRNkcZc
2
1IV/ZhBhMfkaiZPxiwGG2Q5SKD0/Nxcr6iXJSqKFAoGAXZJFJm85AdgcL5tw3JU
A
XRIArNBv+WGv+bVEurlcoDT9RQFvR10/3EvDiPVzcZHTLC1ArT7zv7p6DOQazx5
u
BapULjD0GOO140mcL+NXuKaf0qUFnzufXq3ZS9PXpMuJa5FeG4JQv73WYfKwPNL
v
```

```
9QtAUlophZaKY7sZoHXlkIECgYAWdeqLVZnvAOwShqJSugQZvIbok2sM7yMDk12
o
D69hoZstzjTKeI/6CzuC2MnxyzSpozOuO4fYwstbsSJUVo0GI1tqAuSvQzUPrWw
A
v9iOzvCNxuR4GwLoQYdfXW0wu8GphpzltrJWoTi2f5YgC5CXYReoL2/VZ8R86UM
9
rqnRnQKBgAvWFGBFfOzdGlMET+Ym5HyvzK/at4e2b9TP8qAjMqGpEpVv+pU8c/r
t
Xz1eZNk9ptBIJiPlYaNPNM/75tQ1AMNlg0Sv9RzowsG8EJr5oSIq3xpulLhTFb8
G 1gEARgpDLMdcsHVwjdW7lCCG+cA8ayyo0BVk/WONnUNCGQAMouSn -----END
RSA PRIVATE KEY-----
```

```
Invalid Output :unable to load Private Key
139695916947264:error:0906D06C:PEM routines:PEM_read_bio:no
start line:crypto/pem/pem_lib.c:691:Expecting: ANY PRIVATE KEY
```

Check certificate file format

```
openssl x509 -in DPOD.cer -text -noout
Valid output :
Certificate: Data: Version: 3 (0x2) Serial Number:
ab:36:a9:5c:d4:1d:c3:aa Signature Algorithm:
sha256WithRSAEncryption Issuer: CN = OperationsDashboard
Validity Not Before: May 15 09:09:18 2017 GMT Not After : May
13 09:09:18 2027 GMT Subject: CN = OperationsDashboard Subject
Public Key Info: Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit) Modulus:
00:ea:d8:b6:f5:ab:16:2e:29:0d:1e:68:9c:8b:fd:
92:8e:09:10:5a:37:eb:cf:0e:a7:da:5d:80:43:60:
31:cd:53:c6:c2:7a:32:3c:e1:d6:4f:3e:7e:d0:7f:
96:61:fc:b4:36:04:4d:12:7d:4a:bd:c0:6a:26:d9:
36:e9:c3:38:35:48:60:76:2e:ea:3f:98:35:d6:ef:
f5:9e:41:aa:74:98:8f:2b:70:f1:05:d8:af:60:b9:
c9:11:01:7a:82:f2:b9:ee:7c:d4:1e:41:07:30:b7:
3d:df:34:c9:aa:5f:8e:e5:d5:20:8c:a7:64:1b:f0:
e7:20:83:e5:f6:05:d4:b9:6d:f7:96:8e:55:8d:fb:
6f:32:d7:52:a0:52:09:e1:25:4c:b6:b8:92:4e:61:
3c:08:61:f8:f4:2a:95:bb:4d:d0:a7:98:e1:7c:09:
b3:f3:75:74:ed:07:03:e9:8a:41:7b:d3:03:fd:f7:
44:87:06:3f:63:e9:07:f8:0d:66:05:c8:40:19:30:
cb:2f:3e:ce:f1:ad:85:62:83:07:82:4c:9c:0e:e8:
99:b8:80:62:4b:34:9a:57:a4:df:fe:6c:bc:9f:81:
7c:73:e9:2a:73:67:c5:4e:a1:d9:99:6d:07:f1:d3:
11:8b:64:4d:46:0b:d0:e8:a9:fc:8e:83:7b:4d:eb: f8:c5 Exponent:
65537 (0x10001) X509v3 extensions: X509v3 Subject Key
Identifier:
E7:09:B0:A0:66:32:5F:BD:BF:8E:9E:76:07:02:AB:58:FD:E3:CD:66
X509v3 Authority Key Identifier:
keyid:E7:09:B0:A0:66:32:5F:BD:BF:8E:9E:76:07:02:AB:58:FD:E3:CD:
66 X509v3 Basic Constraints: CA:TRUE Signature Algorithm:
sha256WithRSAEncryption
3a:f3:8b:41:31:77:93:c9:28:85:f0:81:31:5c:fb:19:ad:05:
26:81:98:a7:28:e5:6a:35:04:d3:e5:72:fa:f7:3f:50:42:c1:
c6:32:da:f0:49:6c:31:b4:c3:5a:9c:b4:64:66:67:2f:e3:87:
fe:cc:2c:2f:3b:89:e0:be:6c:c5:be:0a:be:50:e2:cd:40:2f:
90:37:91:8d:4c:48:f6:98:88:53:bc:03:f4:61:70:63:07:5f:
44:dd:8a:8c:9b:d5:5c:d2:cf:b7:35:8b:3d:3a:e2:87:28:67:
40:dc:d6:c2:63:b0:94:29:be:ce:46:28:c0:c5:20:d4:09:a3:
```

```
f7:dc:7d:d1:18:8d:cc:a8:1c:af:dc:6d:c9:47:c5:aa:23:b8:
74:92:77:ab:76:5c:f8:91:8d:f0:2c:3b:ba:35:c7:1f:d6:91:
34:5d:bf:e6:a1:75:bb:4f:56:c8:b1:b8:2d:84:1c:5a:73:24:
e6:9a:dd:7c:06:c3:70:49:2f:22:e4:50:f6:ec:ae:a4:92:20:
07:cd:07:09:c8:81:4f:a2:f9:f7:55:da:72:90:00:a6:09:4b:
7d:b5:58:53:4a:d6:da:08:9e:62:b1:b1:c4:56:34:e1:98:a5:
14:47:4b:1e:60:5a:d5:53:11:d4:c2:c7:84:fc:f6:2d:41:06:
04:e4:e6:ba


Invalid Output :unable to load certificate
```

```
140583261931328:error:0906D06C:PEM routines:PEM_read_bio:no
start line:crypto/pem/pem_lib.c:691:Expecting: TRUSTED
CERTIFICATE
```

Limit Admin Users Access by IP

You can limit admin users' login to a set of IP addresses, this feature is turned off by default.

To enable it:

1. Login to your DPOD as root user
2. Start app-util.sh and stop the UI service via the "Stop Service" menu option (note: this will logoff all existing users)
3. Edit the file /app/ui/MonTier-UI/conf/MonTierUI.conf
4. Search for the configuration property security.limit.admin.ip
5. The property's value may contain:
   blank - turned off, no check will be performed
   a specific IP - like 10.0.0.9
   an IP range surrounded with square brackets - For example 10.0.0.[100-200] , 10.0.[0-220].[0-255] or 128.[10-17].0.5
   a list of IPs and IP ranges, use comma as a separator- 10.0.0.1, 10.0.0.3, 10.0.[10-20].[0-255]

   > Entering an invalid value for the security.limit.admin.ip property will prevent the UI service from starting

6. Save the file
7. Start app-util.sh and start the UI service via the "Start Service" menu option

Role Based Access Control

DPOD uses Role Based Access Control to splice user access to the information available through the system.

User and Group Registries

DPOD supports two types of user and group registries:

- **DPOD's internal database registry**
- **Lightweight Directory Access Protocol (LDAP) user registry**

An installation may choose to use either DPOD's internal database registry or an LDAP user registry.

DPOD's Internal database registry

For ease of use, DPOD uses its internal database registry by default. Within this registry:

- Users and security groups are defined via the Web Console.
- Users may be members of several groups.

For more information, read the Users and Security Groups sections under Security Management.

> This registry should only be used for **non-production** environments or during an evaluation process of DPOD.
>
> For **production** environments, the only supported registry is the LDAP user registry.

LDAP User Registry

DPOD may be configured to use an LDAP user registry. In that case:

- Users and security groups are managed within the LDAP user registry.
- DPOD performs LDAP queries to authenticate users and to assign them with security groups and roles.
- Defining users and security groups is not available via the Web Console.
- The internal database registry is not in use.

Configuring DPOD to use LDAP user registry is described in Configuring LDAP.

Security Roles

Security roles are used to provide a means for the administrator to filter the view users have of the system. Administrators can use the roles to filter out devices, domains, services, client IP addresses, payload and more from a user's view, thereby providing each user with insights to only the parts of the system they are allowed to access.

There are two types of security roles available with DPOD:

- **Built-in Roles** - DPOD's own built-in roles, which can not be added, deleted or altered.
- **Custom Roles** - defined by the administrator. These roles may be added, deleted or altered by a DPOD Administrator.

Built-in roles

Built-in roles are hard-coded, system-provisioned roles that limit access to certain pages of DPOD's Web Console or REST API.

Each user must be assigned to at least one built-in role, or they will not be able to login to the console.

The built-in roles are available for view-only under **[Manage Security Roles]** page (As described in Security Roles).

When using DPOD's internal database registry, users and security groups may be assigned with a built-in role from the Web Console. When using an LDAP user registry, built-in roles are assigned based on LDAP queries.

The table below lists the available built-in roles:

Role Name	Description
OpDashAdminRole	Built-in Administrator role. Provides full access.
OpDashPowerUserRole	Built-in Power User role. Allows access to Dashboards, Investigate, Explore, Reports execution and viewing services configuration.
OpDashOperatorRole	Built-in role for controllers. Allows access to Dashboards, Investigate and Explore views.
OpDashInvestigatorRole	Built-in role for investigators. Allows access to some of the Dashboards and Investigate views.

Custom roles

Custom roles are optional, application-level roles managed by the administrators. They can be used to limit access to certain data such as specific devices, domains, payload etc.

Each custom role is configured with several permission directives that dictate the allowed or denied access to devices, domains, services etc.

A user does not have to be assigned with custom roles. Users that are not assigned with any custom role have access to all the data in the system, as limited by their built-in role.

The custom roles are accessed and managed using the **[Manage System Roles]** page (As described in Security Roles).

Each custom role should be linked to users or groups (defined in DPOD's internal database registry or in the LDAP user registry).

> If you are using an LDAP user registry, please make sure you link custom roles with specific LDAP users or LDAP groups, as describe in Security Roles.

Effective Access Rights

A user may be assigned with several custom roles, directly or via groups. The effective access rights of a user is calculated according to the rules described below:

- If the user has access to certain items (devices/domains/services/client IP addresses), they are denied from all other items of the same type. For example, if a user is allowed access to devices MyDevice1 and MyDevice2, they can only have access to these devices, and are denied from all other devices.
- If the user is denied from certain items, they are allowed to all other items of the same type. For example, if a user is denied from devices MyDevice1 and MyDevice2, they still have access to all other devices.
- If the user is denied from certain items, they will not be able to access them, even if they have access to the same items in other custom roles they are assigned to. For example, if a user is assigned with CustomRole1, which denies access to MyDevice1, and the same user is also assigned with CustomRole2, which provides access to MyDevice1, the user will not have access to MyDevice1.
- If a user is assigned with several custom roles, field values are merged. For example, if a user is assigned with CustomRole3, which provides access to MyDevice3, and the same user is also assigned with CustomRole4, which provides access to MyDevice4, the user will have access to both MyDevice3 and MyDevice4.

CONFIGURING LDAP

DPOD should be configured to use an LDAP user registry. The internal database registry is used only for initial phase for fast system setup.

For Production installation LDAP configuration is the only one supported. When using DPOD with LDAP the following behavior is expected:

- Users and security groups are managed within the LDAP user registry.
- DPOD performs LDAP queries to authenticate users and to assign them with security groups and roles.
- Defining users and security groups is not available via the Web Console.
- The internal database registry is not in use.

In order to configure LDAP, follow the following steps:

- Planning LDAP Configuration
- LDAP Configuration Script
- Troubleshooting

Planning LDAP Configuration

This page lists all the parameters required for LDAP configuration, and possible scenarios.

LDAP Server

DPOD needs details about the LDAP server so it can query the LDAP user registry.

Ensure to have the following details before proceeding with the next configuration steps:

LDAP server IP address	The IP address of the LDAP server
LDAP server port	e.g. 389 or 3268 if using Global Catalog in AD
Referrals	Whether LDAP referrals should be followed or ignored (usually ignored for better performance)
Query user distinguished name (DN) and its password	A user that is used to connect to the LDAP server and perform queries. e.g. cn=LDAP Query User,ou=people,dc=example,dc=org

LDAP Users

To be able to authenticate users, DPOD needs to know what LDAP queries it needs to perform in order to verify usernames and passwords.

The best way to figure this out is to examine user entries within the LDAP server using an LDAP browsing software compatible with your LDAP server.

Ensure to have the following details before proceeding with the next configuration steps:

User search base entry	The location in the LDAP tree where user entries should be searched for. Specific locations have better performance than global ones. e.g. ou=people,dc=example,dc=org
User search sub-tree	Whether user entries should be queried in the entire sub-tree of the user search base entry (usually true).
User search filter	The search filter to use in order to find a user entry based on the login user name, using standard LDAP search filter syntax. Usually the user search filter combines 2 conditions: First filter the entries based on the "objectClass" attribute and then filter the entries based on the login user name. User entries can normally be identified by an "objectClass" of "person", "organizationalPerson" or "inetOrgPerson". The user entry attribute that contains the login user name is usually "uid", "sAMAccountName" or "cn". e.g. (&(objectClass=person)(sAMAccountName={0}))
A user and its password for testing	A real user defined in the LDAP user registry who will be using DPOD - will be used to verify that the configuration is valid.

LDAP Groups

To be able to assign roles to users, DPOD needs to know what LDAP queries it needs to perform in order to fetch the list of groups a user belongs to.

The best way to figure this out is to examine group entries within the LDAP server using an LDAP browsing software compatible with your LDAP server.

Ensure to have the following details before proceeding with the next configuration steps:

Group search base entry	The location in the LDAP tree where group entries should be searched for. Specific locations have better performance than global ones. e.g. ou=groups,dc=example,dc=org
Group search sub-tree	Whether group entries should be queried in the entire sub-tree of the group search base entry (usually true).
Group search nested	Whether group entries can be nested within each other (usually true).

Group search filter	The search filter to use in order to fetch the list of groups a user belongs to once a user has authenticated successfully, using standard LDAP search filter syntax. Usually the group search filter combines 2 conditions: First filter the entries based on the "objectClass" attribute and then filter the entries based on the authenticated user. Group entries can normally be identified by an "objectClass" of "group" or "groupOfUniqueNames". The group entry attribute that contains its members is usually "member" or "uniquemember". e.g. (&(objectClass=groupOfUniqueNames)(uniqueMember={1}))
Group role attribute name	The attribute name at the group entry that contains the role name (usually cn). e.g. cn

Built-in Roles

For security reasons, authenticated users are assigned with built-in roles based on LDAP queries only.
This means, for example, that a user may be granted with Administrator privileges only if it is configured that way in the LDAP user repository.

In order to assign built-in roles to users, DPOD needs to associate a user or a group with its built-in roles using an LDAP entry attribute. There are 2 possible scenarios:

- Scenario A - Define the built-in role name as an attribute of the user entry
- Scenario B - Define the built-in role name as an attribute of the group entry

> **The most common scenario is Scenario B, where the group's name (cn) is used as the group role attribute name.**
> This scenario does not require extending any schemas - only creating groups with pre-defined names. See below for more details.

Scenario A - Define the Built-in Role Name as an Attribute of the User Entry

In this scenario, the LDAP administrator defines an attribute for the user entry (e.g. **DPODRole** attribute) which contains the built-in role name of that user.

- The attribute must be defined in the user class LDAP schema, which means that this schema might need to be extended.
- Add the attribute with one of the built-in role names (e.g. OpDashAdminRole) to each user that should use DPOD's Web Console.
  For example, an administrator user named "john" (cn=john) should have the attribute "DPODRole=OpDashAdminRole".

If you choose this scenario, ensure to have the following details before proceeding with the next configuration steps:

User role attribute name	The attribute name of the user entry that contains the built-in role name of that user. e.g. DPODRole

Scenario B - Define the Built-in Role Name as an Attribute of the Group Entry

In this scenario, the LDAP administrator defines an attribute at the group entry that contains the built-in role name of users that belong to that group.

- The attribute must be defined in the group class LDAP schema, which means that this schema might need to be extended.
  Usually, the built-in role name is stored as the group name (cn), thus avoiding the need to extend the schema.
- Create 4 groups - one for each built-in role. The group names should be identical to the built-in role names if the chosen attribute is the group name (cn).
- Add users to the groups.
  For example, an administrator user named "john" (cn=john) should belong to a group named "OpDashAdminRole" (cn=OpDashAdminRole).

LDAP Configuration Script

DPOD includes an LDAP configuration script for easy configuration of DPOD to use an LDAP user registry.
The script uses a user-provided parameters file with the desired configuration. It verifies the configuration, updates the configuration database and files and restarts the necessary services.

It can also disable the LDAP configuration in order to rollback to the internal database registry.

Please make sure to gather all the information listed in Planning LDAP Configuration, which includes detailed explanation on all the parameters.

Parameters File

A template of the LDAP parameters file is provided at /app/utils/LDAP_parameters.properties.

It is recommended to backup the file before modifying it:

```
cp /app/utils/ldap/LDAP_parameters.properties
/app/utils/ldap/LDAP_parameters.properties.orig
```

Edit the parameters file and set the following parameters **based on the information that was collected in Planning LDAP Configuration**:

Parameter	Description
builtinRoleMethod	Should be "user_attribute" (for scenario A) or "group_attribute" (for scenario B). e.g. group_attribute
testUserName	The user name of a user for testing e.g. adminford
testUserPassword	The password of a user for testing Note: This password is used only for testing and is not stored in the configuration database and files e.g. pass123
connectionUrl	LDAP server URL including port. Use ldap:// prefix for non-SSL connection and ldaps:// prefix for SSL connection. e.g. ldap://192.168.110.15:389
referrals	Whether LDAP referrals should be followed or ignored (follow/ignore) e.g. ignore
connectionName	Query user distinguished name (DN) e.g. cn=LDAP Query User,ou=people,dc=example,dc=org
connectionPassword	Query user password Note: This password will be encrypted and stored in the configuration database and files e.g. pass123
userSearchBase	User search base entry e.g. ou=people,dc=example,dc=org
userSearchSubtree	User search sub-tree (true/false) e.g. true
userSearchFilter	User search filter Use **{0}** as a placeholder for the user name entered in the login screen e.g. (&(objectClass=person)(sAMAccountName={0}))
groupSearchBase	Group search base entry e.g. ou=groups,dc=example,dc=org
groupSearchSubtree	Group search sub-tree (true/false) e.g. true
groupSearchFilter	Group search filter Use **{0}** as a placeholder for the full DN of the user found in the LDAP server e.g. (&(objectClass=groupOfUniqueNames)(uniqueMember={0}))

groupSearchNested	Group search nested (true/false) e.g. true
groupRoleAttributeName	Group role attribute name e.g. cn
userRoleAttributeName	**For scenario A only** User role attribute name e.g. "DPODRole"

Testing LDAP Configuration

In order to test LDAP configuration, use the following command:

```
cd /app/utils/ldap
/app/scripts/app_ldap_utilities.sh -f ./LDAP_parameters.properties
```

Add "-y" or "--assume-yes" to run the test without prompting for confirmation.

For a **valid** LDAP configuration the command's output should be:

```
28/06/2018 15:24:04,283- INFO   Starting LDAP Utilities
28/06/2018 15:24:04,290- INFO   Reading user parameters file,
path=./LDAP_parameters.properties

28/06/2018 15:24:04,293- INFO   This utility is about to connect to the
LDAP registry to test the configuration.
28/06/2018 15:24:04,293- INFO   Please confirm connecting to the LDAP
registry (y,n):
y
28/06/2018 15:24:05,310- INFO   Connecting to the LDAP server,
connectionUrl=ldap://ldap-server:10389
28/06/2018 15:24:05,329- INFO   Connected to LDAP server successfully
28/06/2018 15:24:05,330- INFO   Searching for test user,
testUserName=test
28/06/2018 15:24:05,336- INFO   Test user found successfully,
DN=cn=test,ou=people,dc=example,dc=org
28/06/2018 15:24:05,338- INFO   Connecting to the LDAP server using test
user DN and password
28/06/2018 15:24:05,344- INFO   Connected to LDAP server using test user
DN and password successfully
28/06/2018 15:24:05,345- INFO   Searching for test user groups
28/06/2018 15:24:05,365- INFO   Found 3 test user groups with the group
name attribute
28/06/2018 15:24:05,368- INFO   Searching for a groups attribute since
builtin role method is group_attribute
28/06/2018 15:24:05,476- INFO   Tested LDAP configuration against LDAP
registry successfully
28/06/2018 15:24:05,476- INFO   The operation completed successfully
```

For an **invalid** LDAP configuration, the command's output might be:

```
28/06/2018 15:28:02,902- INFO   Starting LDAP Utilities
28/06/2018 15:28:02,909- INFO   Reading user parameters file,
path=./LDAP_parameters.properties

28/06/2018 15:28:02,912- INFO   This utility is about to connect to the
LDAP registry to test the configuration.
28/06/2018 15:28:02,912- INFO   Please confirm connecting to the LDAP
registry (y,n):
y
28/06/2018 15:28:03,638- INFO   Connecting to the LDAP server,
connectionUrl=ldap://wrong-server:10389
28/06/2018 15:28:06,663- ERROR   The operation failed. See log file for
more details.
```

In case of failure, inspect the log file for detailed failure messages. The log file is located in **/logs/ui/app_ldap_utilities.log**.

Change the LDAP configuration parameters and rerun the script until tests are successful.

Updating LDAP Configuration

Once LDAP configuration has been tested and found valid, use the following command to perform the change in the configuration database and files:

```
cd /app/utils/ldap
/app/scripts/app_ldap_utilities.sh -f ./LDAP_parameters.properties -u
```

Add "-y" or "--assume-yes" to run the update without prompting for confirmation.

> Ensure DPOD's services are up and running before updating the LDAP configuration.

The command output should be:

```
28/06/2018 15:30:50,085- INFO   Starting LDAP Utilities
28/06/2018 15:30:50,093- INFO   Reading user parameters file,
path=./LDAP_parameters.properties

28/06/2018 15:30:50,097- INFO   This utility is about to connect to the
LDAP registry to test the configuration.
28/06/2018 15:30:50,097- INFO   Please confirm connecting to the LDAP
registry (y,n):
y
28/06/2018 15:30:51,915- INFO   Connecting to the LDAP server,
connectionUrl=ldap://ldap-server:10389
28/06/2018 15:30:51,932- INFO   Connected to LDAP server successfully
28/06/2018 15:30:51,933- INFO   Searching for test user,
testUserName=test
```

```
28/06/2018 15:30:51,938- INFO   Test user found successfully,
DN=cn=test,ou=people,dc=example,dc=org
28/06/2018 15:30:51,939- INFO   Connecting to the LDAP server using test
user DN and password
28/06/2018 15:30:51,944- INFO   Connected to LDAP server using test user
DN and password successfully
28/06/2018 15:30:51,945- INFO   Searching for test user groups
28/06/2018 15:30:51,955- INFO   Found 3 test user groups with the group
name attribute
28/06/2018 15:30:51,956- INFO   Searching for a groups attribute since
builtin role method is group_attribute
28/06/2018 15:30:52,006- INFO   Tested LDAP configuration against LDAP
registry successfully

28/06/2018 15:30:52,006- INFO   This utility is about to update the UI
service configuration to work with LDAP registry.
28/06/2018 15:30:52,007- INFO   To apply the new configuration, the UI
service will be restarted afterwards.
28/06/2018 15:30:52,008- INFO   Please confirm the configuration update
(y,n):
y
28/06/2018 15:30:53,586- INFO   Enabling LDAP configuration in database
28/06/2018 15:30:53,949- INFO   Enabled LDAP configuration in database
successfully
28/06/2018 15:30:53,951- INFO   Creating a backup of UI server
configuration file server.xml,
backupFilePath=/app/ui/MonTier-UI/conf/server.xml.2018-06-28-153053
28/06/2018 15:30:53,957- INFO   Created a backup of UI server
configuration file server.xml successfully
28/06/2018 15:30:53,958- INFO   Enabling LDAP configuration in UI server
configuration file server.xml
28/06/2018 15:30:54,036- INFO   Enabled LDAP configuration in UI server
configuration file server.xml successfully

28/06/2018 15:30:54,037- INFO   To apply the new configuration, the UI
service needs to be restarted.
28/06/2018 15:30:54,037- INFO   Please confirm the UI service restart
(y,n):
y
```

```
28/06/2018 15:30:56,345- INFO   Restarting UI server
28/06/2018 15:30:56,630- INFO   Restarted UI server successfully
28/06/2018 15:30:56,630- INFO   The operation completed successfully
```

Disabling LDAP Configuration

Use the following command to disable LDAP configuration in System Parameters:

```
cd /app/utils/ldap
/app/scripts/app_ldap_utilities.sh -d
```

Add "-y" or "--assume-yes" to run the update without prompting for confirmation.

> Ensure DPOD's services are up and running before disabling the LDAP configuration.

The command output should be:

```
28/06/2018 15:36:08,878- INFO   Starting LDAP Utilities

28/06/2018 15:36:08,897- INFO   This utility is about to update the UI
service configuration to work with its local user registry.
28/06/2018 15:36:08,897- INFO   To apply the new configuration, the UI
service will be restarted afterwards.
28/06/2018 15:36:08,897- INFO   Please confirm the configuration update
(y,n):
y
28/06/2018 15:36:12,465- INFO   Disabling LDAP configuration in database
28/06/2018 15:36:12,711- INFO   Disabled LDAP configuration in database
successfully
28/06/2018 15:36:12,713- INFO   Creating a backup of UI server
configuration file server.xml,
backupFilePath=/app/ui/MonTier-UI/conf/server.xml.2018-06-28-153612
28/06/2018 15:36:12,725- INFO   Created a backup of UI server
configuration file server.xml successfully
28/06/2018 15:36:12,726- INFO   Disabling LDAP configuration in UI
server configuration file server.xml
28/06/2018 15:36:12,808- INFO   Disabled LDAP configuration in UI server
configuration file server.xml successfully

28/06/2018 15:36:12,808- INFO   To apply the new configuration, the UI
service needs to be restarted.
28/06/2018 15:36:12,810- INFO   Please confirm the UI service restart
(y,n):
y
28/06/2018 15:36:13,625- INFO   Restarting UI server
28/06/2018 15:36:16,792- INFO   Restarted UI server successfully
28/06/2018 15:36:16,793- INFO   The operation completed successfully
```

Manually Inspecting LDAP Configuration

Inspecting LDAP Configuration in Configuration File (server.xml)

Edit the server configuration file and look for the **LDAPRealm** element. This element contains all the configuration set automatically by the script.

```
vi /app/ui/MonTier-UI/conf/server.xml
```

Inspecting LDAP Configuration in System Parameters

Open the Web Console and navigate to System Parameters page **[Manage System System Parameters].**

The LDAP configuration system parameters are listed under "LDAP" category.

Troubleshooting

The information in this page can be used to help troubleshoot LDAP issues.

Debugging

Enabling UI Service LDAP Trace

To enable trace logging edit the UI service log4j configuration file : /app/ui/MonTier-UI/lib/log4j2.xml

Change the "MNTR_CUSTOM_ROLES" logger to level="trace" as describe below :

```
<Logger name="MNTR_CUSTOM_ROLES" level="trace" additivity="false">
  <AppenderRef ref="LDAPLOG"/>
</Logger>
```

The output log file will be created in the UI service log directory : /logs/ui with the name ldapLog.log

Common Issues

Referrals

You might get the following error message:

> An exception performing authentication javax.naming.PartialResultException: Unprocessed Continuation Reference(s); remaining name 'DC=XX,DC=XX,DC=XX'

The issue may be resolved by changing the referrals parameter (both inside the server.xml file and system parameters) to "ignore" and connecting to the greater AD "forest", which acts like a regular LDAP server on port 3268 (or 3269 for LDAPS).

LDAP authentication error codes

See the following link: http://www-01.ibm.com/support/docview.wss?uid=swg21290631

Web Console Audit Log

The Web Console audit records are written to the product's UI component log files.

The audit records include the following information:

Value	Description
Time stamp	The time stamp that an action was done. For example: 05/02/2017 18:18:30,839
Action execution time (ms)	The action execution time in milliseconds.
User IP Address	The IP address of the user that performed the action (for customers over NAT the actual IP may be the NAT service)
User ID	The DPOD logged in user ID that performed the action
Action	The action description. For example: addUser(userName=User1)

ENABLING AUDIT LOG

To enable audit logging, edit the UI service log4j configuration file: /app/ui/MonTier-UI/lib/log4j2.xml.

1. Add a new appender under <Appenders> element with the following content:

```
<RollingFile name="AUDIT" fileName="${tomee-log-path}/audit.log"
filePattern="${tomee-log-path}/audit.%i.log" append="true"
bufferedIO="false" bufferSize="0">
 <PatternLayout>
  <Pattern>%d{dd/MM/yyyy HH:mm:ss,SSS}- %p %c{1.} [%t] %m
%ex%n</Pattern>
 </PatternLayout>
 <Policies>
  <SizeBasedTriggeringPolicy size="5 MB" />
 </Policies>
  <DefaultRolloverStrategy max="10"/>
</RollingFile>
```

2. Add a new logger under <Loggers> element with the following content:

```
<Logger name="org.montier.ui.web.filters.AuditFilter" level="debug"
additivity="false">
 <AppenderRef ref="AUDIT"/>
</Logger>
```

Make sure to restart the UI service after altering the log4j configuration file.

The output log file will be created in the UI service log directory (/logs/ui) with the name audit.log

In order to export the audit records to an external system, use file transfer mechanism (scp) to copy the logs off the product's server.

AUDIT RECORDS EXAMPLE

```
05/06/2018 18:18:30,839- DEBUG o.m.u.w.f.AuditFilter
[ajp-bio-8070-exec-1]   51    192.168.65.190  admin
getSystemParameters()
05/06/2018 18:18:34,183- DEBUG o.m.u.w.f.AuditFilter
[ajp-bio-8070-exec-1]   8     192.168.65.190  admin           getUsers()
05/06/2018 18:18:46,277- DEBUG o.m.u.w.f.AuditFilter
[ajp-bio-8070-exec-1]   40    192.168.65.190  admin
addUser(userName=User1)
05/06/2018 18:18:46,304- DEBUG o.m.u.w.f.AuditFilter
[ajp-bio-8070-exec-1]   8     192.168.65.190  admin           getUsers()
```

Product Components

The following sections describe how security is deployed and configured for the various DPOD components.

- Syslog Agents Security
- WS-M Agents Security
- Big Data Store
- Monitored Device Interface
- Configuration Files

Syslog Agents Security

DPOD Syslog agents use TCP (not UDP) in order to deliver reliable connection. The agents do not use an encrypted tunnel (SSL / TLS).

To use an encrypted tunnel, the organization may use external tools to proxy DPOD agents (E.g. the open source tool https://www.stunnel.org/index.html - GNU GPL license)

WS-M Agents Security

DPOD WS-M (WS-Management) agents receive HTTP requests over TCP connection. Secure tunneling is currently not supported.

Big Data Store

The Big Data store components (Nodes) communicate between them. The components do not authenticate each other.

When deploying DPOD All-In-One appliance, all communication between the big data store components is done internally making the authentication between components less significant security wise.

When deploying DPOD in a distributed architecture we highly recommend restrict access to big data store components using network security components like firewall.

Monitored Device Interface

XML MANAGEMENT INTERFACE

DPOD communicates with the monitored appliances using the SOMA (SOAP configuration Management).

All SOMA communication is made over secure tunnel (SSL /TLS) and involves authenticating to the monitored device.

The device user account does not have to be privileged user. For needed specification see next section (DPOD user account).

ADD SSL CLIENT AUTHENTICATION SUPPORT FOR PRODUCT COMPONENTS

A user may configure the DataPower's XML Management Interface to require clients to authenticate during the SSL handshake using client certificate (SSL Client-Authentication).

In order for DPOD components to authenticate to DataPower's XML Management Interface using client certificate, a dedicated configuration is needed to use a KeyStore that contains the client certificate.

Use the following procedure to configure DPOD's components for SSL Client-Authentication:

1. Login to DPOD's CLI using SSH.
2. Use the "Keytool" utility to create a new JKS (Java KeyStore) :

   ```
   keytool -genkey -alias temp -keystore "/tmp/dpod_custom.jks"
   ```

   A default alias is required for the Keytool to create the JKS.
   This alias will be called "temp" since it is not needed by the product and will be deleted after the JKS creation.

3. Keytool will ask a series of questions in order to create the "temp" alias and the JKS:
   Answer the questions as you wish :

   ```
   Enter keystore password:
   Re-enter new password:
   What is your first and last name?
     [Unknown]:  FirstName
   What is the name of your organizational unit?
     [Unknown]:  LastName
   What is the name of your organization?
     [Unknown]:  SomeOrg
   What is the name of your City or Locality?
     [Unknown]:
   What is the name of your State or Province?
     [Unknown]:
   What is the two-letter country code for this unit?
     [Unknown]:
   Is CN=FirstName, OU=LastName, O=SomeOrg, L=Unknown, ST=Unknown,
   C=Unknown correct?
     [no]:  yes

   Enter key password for <temp>
           (RETURN if same as keystore password):
   Re-enter new password:
   ```

4. As the alias is not required by the product, delete the alias from the JKS:

   ```
   keytool -delete -alias temp -keystore "/tmp/dpod_custom.jks"
   ```

   Make sure that the JKS is now empty:

```
keytool -list -v -keystore "/tmp/dpod_custom.jks"
```

The output should resemble the following:

```
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 0 entries
```

5. Convert the certificate (.cer file) and the private key (.pem file) to a pkcs12 file, using the openssl tool :

```
openssl pkcs12 -export -in <cer file> -inkey <pem file> >
/tmp/TempKeyStore.p12
```

The user will be asked to enter a password for the new pkcs12 keystore.
Verify that the pkcs12 keystore contains one entry :

```
keytool -list -v -keystore "/tmp/TempKeyStore.p12"
```

The output should begin with the following lines :

```
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: 1
Creation date: Aug 28, 2017
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
```

6. Import the key and certificate from the p12/pfx file to the JKS :

```
keytool -importkeystore -srckeystore /tmp/TempKeyStore.p12
-srcstoretype pkcs12 -destkeystore /tmp/dpod_custom.jks
-deststoretype JKS
```

The user will be asked to enter both the source and destination keystores passwords.

The output should look like :

```
Enter destination keystore password:
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0
entries failed or cancelled
```

7. Move the JKS to the correct directory :

```
mkdir -p /app/custom/certs
mv /tmp/dpod_custom.jks /app/custom/certs
```

8. Add the new KeyStore to product components activation parameters

   The following product services need to updated to use the new JKS :

   /etc/init.d/MonTier-UI
   /etc/init.d/MonTier-HK-WdpDeviceResources
   /etc/init.d/MonTier-HK-SyslogKeepalive
   /etc/init.d/MonTier-HK-WdpServiceResources
   /etc/init.d/MonTier-HK-WsmKeepalive
   /etc/init.d/MonTier-HK-ESRetention
   /etc/init.d/MonTier-Reports

   Add the following line to each of the files above :

```
APP_JAVA_OPTS="$APP_JAVA_OPTS -Djavax.net.debug=ssl
-Djavax.net.ssl.keyStoreType=jks
-Djavax.net.ssl.keyStore=/app/custom/certs/dpod_custom.jks
-Djavax.net.ssl.keyStorePassword=<Your_JKS_Password>"
```

> Replace "Your_JKS_Password" with the password that you have given to the JKS keystore.
>
> The line should be added to the lines marked with the remark "JVM Settings" (look for the lines containing "APP_JAVA_OPTS=$APP_JAVA_OPTS").

9. Restart the product, using app-util.sh

Configuration Files

The following sections provide details of DPOD's configuration files.

- Application Server DataBase Password
- Derby DataBase CLI (ij)

APPLICATION SERVER DATABASE PASSWORD

DERBY DATABASE CLI (IJ)

Virtual Appliance Security

CLI ACCESS

DPOD virtual appliances are based on Linux OS and can be accessed via SSH (port 22).

Since DPOD Console provides all functionality needed by the end user, you will normally only need to access DPOD appliance via CLI for special administration purposes such as initial installation, browsing system logs, administrative configuration change (e.g changing certificates) etc.

The root user password is determined by the system administration during DPOD's Appliance Installation process.

The SSH service configuration comply with common security best practice and may be altered by the administrator.

> Modification of the SSH service configuration is not recommended and should only be performed in special cases

OPERATING SYSTEM PASSWORDS RESTRICTIONS

New Operating System users password restrictions comply with common security best practice and may be altered by the administrator.

> Modification of the Password Restirctions is not recommended and should only be performed in special cases

Internal Firewall

DPOD appliances use embedded host based firewall (Linux Iptables). All inbound and outbound communication is blocked with the following exceptions required for the DPOD product.

The communication rules are detailed in the Firewall Requirements topic.

The system administrator may choose to allow additional communication. The DPOD appliance includes a shell script for altering the firewall rules.

Display current firewall rules

Use the following built-in command to display DPOD's default firewall state

```
iptables -L
```

The output is :

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state
RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere            state NEW
tcp dpt:ssh
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ntp
ACCEPT     udp  --  anywhere             anywhere            udp
dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpts:60000:60009
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpts:60020:60029
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:https
REJECT     all  --  anywhere             anywhere            reject-with
icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  anywhere             anywhere            reject-with
icmp-host-prohibited


Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:5550
ACCEPT     udp  --  anywhere             anywhere            udp dpt:ntp
ACCEPT     udp  --  anywhere             anywhere            udp
dpt:domain
CCEPT     tcp  --  anywhere             anywhere            tcp
dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:ldap
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:ldaps
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:msft-gc
ACCEPT     tcp  --  anywhere             anywhere            tcp
dpt:msft-gc-ssl
```

It is recommended to alter this rules using DPOD firewall update tool in order to limit access only to allowed IPs. (e.g. replace the rule that allows every IP to connect to DPOD using tcp port 60000 (syslog) to specific monitored device IP address / monitored device subnet).

ALTERING THE FIREWALL RULES

DPOD installation includes a mechanism for altering the internal firewall rule and resetting it back to default (if needed).

Consult the pages below for more information.

- Firewall Rules Configuration File
- Altering the Firewall Configuration

Firewall Rules Configuration File

DPOD includes a default firewall configuration rules file with a simple format.

```
/app/scripts/app_fw_default_rules
```

The firewall rules configuration file has a very simple format:

- Direction
  - in – for inbound traffic
  - out – for outbound traffic
- type
  - tcp
  - udp
- IP – source ip address
  - Specific IP – 1.1.1.1
  - CIDR range – 1.1.1.0/24, 0.0.0.0/0
- Port – destination port
  - Specific port – 443, 60000
  - Range – 60000:60009

Notes :

- For remark use # sign
- Do not leave empty lines.

DPOD installation includes default rules file located in :

Altering the Firewall Configuration

The following script enables the user to update the internal firewall rules based on the configuration file.

The script supports the following option:

- --applyrules - Will read rules configuration file and apply them overwriting current firewall rules.

  ```
  • app_fwconf.sh --applyrules /app/scripts/app_fw_default_rules
  ```

- --testrules – will apply the rules configuration file for 60 seconds in order to test new rule. After 60 seconds the firewall will revert to default CentOS rules (SSH and ICMP only)
- --reset – firewall rules will be reset to the default CentOS rules (SSH and ICMP only)

Firewall Requirements

This section details the port configuration setup required between DPOD and the your network components.

From	To	Ports (Defaults)	Protocol	Usage
DPOD Appliance	Each Monitored Device	5550 (TCP)	HTTP/S	Monitored Device administration management interface
DPOD Appliance	DNS Server	TCP and UDP 53	DNS	DNS services
DPOD Appliance	NTP Server	123 (UDP)	NTP	Time synchronization
DPOD Appliance	Organizational mail server	25 (TCP)	SMTP	Send reports by email
DPOD Appliance	LDAP	TCP 389 / 636 (SSL). TCP 3268 / 3269 (SSL)	LDAP	Authentication & authorization. Can be over SSL
NTP Server	DPOD Appliance	123 (UDP)	NTP	Time synchronization
Each Monitored Device	DPOD Appliance	60000-60009 (TCP)	TCP	SYSLOG Data
Each Monitored Device	DPOD Appliance	60020-60029 (TCP)	HTTP/S	WS-M Payloads
FROM Users IPs	DPOD Appliance	443 (TCP)	HTTP/S	Access to with IBM DataPower Operations Dashboard Console
FROM Admins IPs	DPOD Appliance	22 (TCP)	TCP	SSH

Special consideration for Docker container Light Development Edition:

Based on the DPOD Docker run command - setup the needed port configuration to communicate with the Docker host (The Docker host is the server with the Docker engine that runs the DPOD container. referred to on the DPOD Docker documentation as **`DPOD_EXT_HOST_IP`**) .
The values in the following table are based on the documentation defaults.

From	To	Ports (Defaults)	Protocol	Usage
DPOD Docker host	Each Monitored Device	5550 (TCP)	HTTP/S	Monitored Device administration management interface
DPOD Docker host	Organizational mail server	25 (TCP)	SMTP	Send reports by email
Each Monitored Device	DPOD Docker host	60000-60009 (TCP)	TCP	SYSLOG Data
Each Monitored Device	DPOD Docker host	60020-60029 (TCP)	HTTP/S	WS-M Payloads
FROM Users IPs	DPOD Docker host	443 (TCP)	HTTP/S	Access to with IBM DataPower Operations Dashboard Console
FROM Admins IPs	DPOD Docker host	9022 (TCP)	TCP	SSH

External Self Service Console

An DPOD External Self-service Console ("DPOD External Self-Service") is an instance of DPOD All-In-One appliance that is deployed externally to a network, provides users with a Console UI only, **and does not store any data of its own**. In lieu of storing data, this instance communicates with an internal DPOD Console ("DPOD Internal Console").

A typical use for an DPOD External Self-Service is to proxy the DPOD Console UI to a less secured network (e.g. a DMZ) without placing DPOD's internal Data Base in that area.

Security note: In the current version of DPOD External Self-Service, the connection to the internal data base is not protected using authentication mechanism. Consider this when planning your deployment and use additional security measures to protect network access to the internal data base.

INSTALLATION PREPARATION

Gather & Prepare Network

1. Ensure you have an IP for the DPOD external Self-service console (including DNS, Default GW, subnet mask and other network configuration).
2. Ensure you have an NTP server available and obtain the NTP server IP address.
3. Ensure the ports detailed below are opened during or after install

From	To	Ports (Defaults)	Protocol	Usage
FROM DPOD External Self-Service	NTP Server	123	NTP	Sync time between DPOD instances
FROM DPOD External Self-Service	Organizational mail server	25	SMTP	Send reports by email
NTP Server	DPOD External Self-Service	123	NTP	Sync time
FROM Users IPs	DPOD External Self-Service	80 ,443	HTTP/s	Work with DPOD Service Center Console
FROM Admins IPs	DPOD External Self-Service	22	TCP	SSH
FROM DPOD External Self-Service	DPOD Internal Console	9302	TCP	Connection to elastic Search Node

Hardware Requirements

Resource	Requirements
Storage	• Disk 1 (for OS): 40GB • Disk 2 (for product installation): 40GB • Disk 3 (Date): minimum 5GB
Memory	Minimum of 32GB reserved
CPU	Minimum 4 cores (2 virtual sockets, with 2 virtual cores each, reserved)
Network	• 1 network interface for the UI • (Optional) - a second network interface to separate DPOD's External Self Service access to the internal database from the UI interface.
Hypervisor	VMWare ESX 5.x

DPOD EXTERNAL SELF-SERVICE POST INSTALLATION TASKS

1. Stop DPOD components
2. Ensure all components are down
3. Disable all DPOD services except Derby, UI and Reports
   a. Edit (with vi) /etc/sysconfig/MonTier and find the line starting with

```
SERVICES_FIRST_GROUP="MonTier-Derby
MonTier-es-raw-trans-Node-1"
```

and remove all components except for MonTier-Derby:

```
SERVICES_FIRST_GROUP="MonTier-Derby"
```

b. Comment out the following lines:

```
SERVICES_SECOND_GROUP="MonTier-es-raw-trans-Node ..."
SERVICES_THIRD_GROUP="MonTier-HK-ESRetention" ...
SERVICES_FORTH_GROUP="MonTier-AggAgent- ..."
SERVICES_FIFTH_GROUP="MonTier-BalancerAgent ..."
SERVICES_SIXTH_GROUP="MonTier-WsmAgent-1 ..."
```

c. Change

```
SERVICES_SEVENTH_GROUP="MonTier-UI MonTier-Reports
MonTier-HK-WsmKeepalive MonTier-HK-SyslogKeepalive"
```

to remove all components except MonTier-UI and MonTier-Reports

```
SERVICES_SEVENTH_GROUP="MonTier-UI MonTier-Reports"
```

4. Change DPOD's Elastic Search alias entry in /etc/hosts to direct to the internal console:

```
vi /etc/hosts
```

Change the line that directs montier-es to point to the internal Console IP Address (1.1.1.1 in the example below)

```
1.1.1.1     montier-es
```

5. Edit DPOD UI configuration file:

```
vi /app/ui/MonTier-UI/conf/MonTierUI.conf
```

and change the port on the following line

```
elasticsearch.discovery.zen.ping.unicast.hosts=montier-es[9300]
```

to the new port

```
elasticsearch.discovery.zen.ping.unicast.hosts=montier-es[9302]
```

6. Comment out the following lines:

```
elasticsearch.node.name=MonTier-UI
elasticsearch.network.host=montier-es-http
elasticsearch.transport.tcp.port=9320
elasticsearch.http_node.host=montier-es-http
elasticsearch.http_node.port=9200
```

7. Update the SystemParameter SQL table:

```
UPDATE SystemParameter
SET value='false'
WHERE name='agents.management.enabled';
```

8. Update the SystemParameter SQL table:

```
UPDATE SystemParameter
SET value='false'
WHERE name = 'system.internal_self_service.is_internal';
```

9. If you wish to let the external self service users access the DevOps Services Portal, change the following system parameters in the external self service console:
a. Internal Self Service Address - enter the address of the internal self service portal
b. Internal Self Service User Name - the DPOD user name that will be used to access the internal portal - it is recommended to create a new user for this purpose
c. Internal Self Service Password - the password for the user that will be used to access the internal portal
d. Internal Self Service Webserver Port - (defaults to 443) the webserver port for the internal self service portal - change this value only if advised.

DPOD INTERNAL CONSOLE POST INSTALLATION TASKS

Connect to the DPOD Internal Console server and alter the configuration to let it accept communication from the DPODExternal Self-Service console.

1. Stop DPOD components
2. Ensure all components are down :
3. Change DPOD ElasticSearch alias entry in /etc/hosts to bind to external IP address

```
vi /etc/hosts
```

and change the line

```
127.0.0.1   montier-es
```

to DPOD's internal console IP address (e.g. 1.1.1.1)

```
1.1.1.1     montier-es
```

4. Start DPOD components
5. Ensure all required components are up (all but "MonTier-AggAgent-1-xxx" and “MonTier-BalancerAgent-1-xxx”)

```
check_status.sh -a
```

DPOD EXTERNAL SELF-SERVICE POST INSTALLATION CHECKS

To verify the DPOD External Self-Service installation, start the External console and ensure all is working as expected.

1. Start DPOD components
2. Ensure all required components are up:

   The following components must be running:
   a. MonTier-Derby
   b. MonTier-UI
   c. MonTier-Reports

3. Enure the UI components is up using ElasticSearch Client mode connection.
   Inside the UI log file at /logs/ui/ MonTier-UI.log locate the following line:

```
04/04/2016 06:55:53,941- DEBUG o.m.c.u.e.ElasticSearchClient
[montier-ui-server-startStop-1] Connecting to ElasticSearch as
transport client
```

4. Basic Installation Verification
   a. Start DPOD's console and sign in: http://<DPOD Server>/
   b. Ensure the System Overview dashboard contains data
   c. Ensure the Investigate screen contains data.

Operating System Users

DPOD's services must run as the "root" user.

The administrator can add additional operating system users but all DPOD's administration should be done when logged in as "root" user.

The administrator can both login as "root" or login as a different user and then switch to the "root" user using "su -" command:

```
su -
```

High Availability, Resiliency or Disaster Recovery

High Availability (HA), Resiliency or Disaster Recovery (DR) Implementation

There are multiple methods available to achieve DPOD HA/DR planning and configuration. These methods are determined based on the customer's requirements, implementation and infrastructure.

Terminology

Node State/mode - A DPOD node can be in one of the following states: **Active** (On, performing monitoring activities), **Inactive** (Off, not performing any monitoring activities), **DR Standby** (On, not performing monitoring activities).

Primary Node - A DPOD installation that actively monitors DataPower instances under normal circumstances (Active state).

Secondary Node - A DPOD installation, identical to the Primary Node (In shared storage scenario it is the same image as the primary node) - that is in DR Standby or Inactive state.

3rd party DR software - A software tool that assists in the process of identifying when the primary node state has changed from *active* to *inactive* and initiates the process of launching the secondary node as active .

DPOD Scalability vs. HA/DR

The DPOD architecture supports installation of multiple DPOD nodes for scalability - to support high throughput in cases of high rate of transactions per second (TPS). However, this does not provide a solution for HA/DR requirements.

For simplicity, this document assumes that only one DPOD node is installed, but the same scenarios and considerations apply for multiple nodes installations.

Important HA/DR Considerations

Consult your BCP/DR/System/Network Admin and address the following questions before selecting which method(s) of HA/DR implementation with DPOD to use:

1. For large installations, DPOD can capture vast volumes of data. Replicating that much data for DR purposes may consume significant network bandwidth, and may incur 3rd party storage replication license costs.

> *Is it cost effective to replicate DPOD's data, or is it acceptable to launch another instance of DPOD with configuration replication only?*

2. The software used for Active/Passive scenario:

> *Will you run DPOD on a virtual infrastructure like VMware, or can you use VMware VMotion or Active/Passive cluster management tools that can help identify and relaunch DPOD on a different cluster member?*

3. You are expected to have an Active/Passive software or another mechanism in place to identify when a DPOD node becomes inactive, and launch a new one in an active cluster member.

> *Do you have such a tool (DR software)?*

4. When launching a new DPOD instance on the backup cluster member:

> *Will the new instance keep the same network configuration of the primary instance (for example: IP Address, DNS, NTP, LDAP, SMTP) or will the configuration change?*

5. Some DataPower architecture solutions (Active/Passive or Active/Active) effect DPOD configuration. If the DataPower IP address changes - then your DPOD configuration may need to change.

> *Does your DataPower architecture use an active/passive deployment? If so - will the passive DataPower have the same IP address when it switches to active?*

Common Scenarios for DPOD HA/DR Implementation

SCENARIO A: ACTIVE/PASSIVE - DPOD'S IP ADDRESS REMAINS THE SAME - SHARED STORAGE

Assumptions:

1. The customer has DataPower appliances deployed using either an Active/Passive, Active/Standby or Active/Active configuration. All DataPower appliances in any of these configurations have unique IP addresses.
2. The customer has storage replication capabilities to replicate DPOD disks based on the disks' replication policy described above.
3. A primary DPOD node is installed, and is configured to monitor all DataPower appliances (active, standby and passive). The secondary node will use the same disks on shared storage.
4. All DPOD network services (NTP, SMTP, LDAP etc.) retain the **same** IP addresses in a failover event (or else a post configuration script is required to be run by the DR software).
5. The customer has a 3rd party software tool or scripts that can:
    a. Identify unavailability of the primary DPOD node.
    b. Launch a secondary DPOD node **using the same IP address as the primary one (usually on a different physical hardware).**
6. The secondary DPOD node is not operating when business is as usual, as disks replication is required and the secondary node has the same IP address as the primary DPOD node.
7. This scenario might not be suitable for high load implementations, as replication of DPOD data disk might not be acceptable.

During a disaster:

1. The customer's DR software should Identify a failure in the DPOD primary node (e.g. by pinging an access IP, sampling the user interface URL or both).
2. The customer's DR software should launch the secondary DPOD node using the same IP address as the failed primary node (or initiate changing the IP address if not already configured that way).

DPOD will be available in the following way:

- As the secondary DPOD node has the same IP address, all DataPower appliances will be able to access it.
- Since all DataPower appliances will have the same IP addresses - DPOD can continue to sample them.
- Since the secondary DPOD node has the same IP address as the primary one, access to DPOD's console retains the same URL.

SCENARIO B: ACTIVE/PASSIVE – DPOD'S IP ADDRESS CHANGES - SHARED STORAGE

Assumptions:

1. The customer has DataPower appliances deployed using either an Active/Passive or Active/Stand-by configuration. All DataPower appliances in any of these configurations have unique IP addresses.
2. The customer has storage replication capabilities to replicate DPOD disks based on the disks' replication policy described above.
3. A primary DPOD node is installed, and is configured to monitor all DataPower appliances (active, standby and passive). The secondary node will use the same disks on shared storage.
4. All DPOD network services (NTP, SMTP, LDAP etc.) retain the **same** IP addresses in a failover event (or else a post configuration script is required to be run by the DR software).
5. The customer has a 3rd party software tool or scripts that can:
    a. Identify unavailability of the primary DPOD node.
    b. Launch a secondary DPOD node **using a different IP address to the primary one (usually on a different physical hardware).**
6. The secondary DPOD node is not operating when business is as usual, since disks replication is required.
7. This scenario might not be suitable for high load implementations, as replication of DPOD data disk might not be acceptable.

During a disaster:

1. The customer's DR software should Identify a failure in DPOD's primary node (e.g. by pinging an access IP, sampling the user interface URL or both).
2. The customer's DR software should launch the secondary DPOD node using a different IP address to the failed primary node (or initiate changing the IP address if not already configured that way).
3. The customer's DR software should execute a command/script to change DPOD's IP address.
4. The customer's DR software should change the DNS name for the DPOD node's web console to reference an actual IP address or use an NLB in front of both DPOD web consoles.
5. The customer's DR software should disable all DPOD log targets, update DPOD host aliases and re-enable all log targets in all DataPower devices. This is done by invoking a REST API call to DPOD.
   (See "refreshAgents" API under Devices REST API).

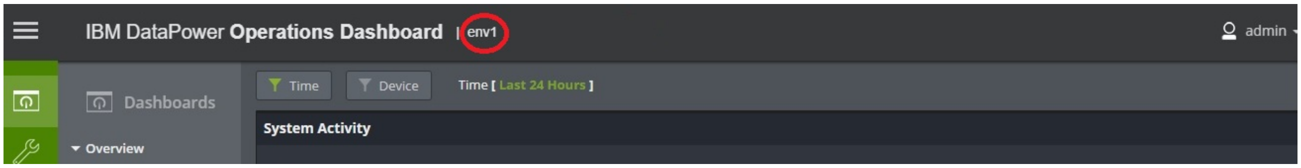
DPOD will be available in the following way:

- Although the secondary DPOD node has a different IP address, all the DataPower appliances will still be able to access it since their internal host aliases pointing to DPOD will be replaced (step 5 above).
- As all DataPower appliances retain the same IP addresses - the secondary DPOD node that was just made active can continue to sample them.
- Although the secondary DPOD node has a different IP address, all users can access DPOD's web console because its DNS name has been changed or it is behind an NLB (step 4 above).

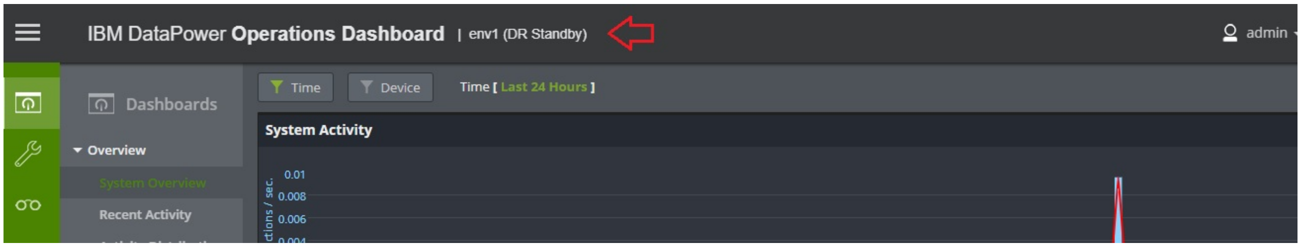
SCENARIO C: ACTIVE/STANDBY – TWO SEPARATE DPOD INSTALLATIONS WITH NO SHARED STORAGE

Assumptions:

1. The customer has DataPower appliances deployed using either an Active/Passive or Active/Stand-by configuration. All DataPower appliances in any of these configurations have unique IP addresses.
2. Two DPOD nodes are installed (requires DPOD version 1.0.5 +), one operates as the Active node and the other one as Standby. After installing the secondary DPOD node, it **must be** configured to run in Standby state. See "makeStandby" API under DR REST API.
3. Both DPOD nodes should have the same environment name. The environment name is set by the customer during DPOD software deployment or during upgrade, and is visible in the top navigation bar (circled in red in the image below):



4. When the DPOD node is in a DR Standby mode, a label is displayed next to the environment name in the Web Console. A refresh (F5) may be required to reflect recent changes if the makeStandby API has just been executed, or when the DPOD status has changed from active to standby or vice versa. See the image below:



5. **As both nodes are up, no configuration or data replication can exist in this scenario.** The customer is expected to configure each DPOD node as a standalone including all system parameters, security groups / roles/ LDAP parameters/ Certificates, custom reports and reports scheduling, custom alerts and alerts scheduling, maintenance plan and user preferences. DPOD is not performing any configuration synchronization.
6. Importantly, the customer must add DataPower instances to each installation in order to monitor all DataPower Devices (active, standby and passive). Starting with DPOD v1.0.5 a new REST API may be utilized to add a new DataPower device to DPOD without using the UI (see Devices REST API). The customer must add DataPower instances to the standby DPOD node and set the agents for each device from the Device Management page in the web console (or by using the Devices REST API). Setting up the devices in the standby DPOD node **will not** make any changes to the monitored DataPower devices (no log targets, host aliases or configuration changes will be made).
7. All DPOD network services (NTP, SMTP, LDAP etc.) have the same IP addresses.
8. The customer has a 3rd party software tool or scripts that can:
    a. Identify unavailability of the primary DPOD node.
    b. Change the state of the secondary node (that is in standby state) to Active state
9. The standby DPOD node can still be online as disk replication is not required.
10. This scenario will not provide High Availability for data. To load data from the Primary node, the customer is required to restore backups taken from primary nodes.
11. During state transition of the Secondary DPOD from Active back to Standby there might be some data loss.

During a disaster:

1. The customer's DR software should Identify a failure in DPOD primary node (e.g. by pinging an access IP, sampling the user interface URL or both).
2. The customer's DR software should enable the standby DPOD node by calling the "standbyToActive" API (see DR REST API). This API will point DPOD's log targets and host aliases of the monitored devices to the standby node and enable most timer based services (e.g. Reports, Alerts) on the secondary nodes.
3. The customer's DR software should change the DNS name for the DPOD node's web console to reference an actual IP address or use an NLB in front of both DPOD web consoles.

DPOD will be available in the following way:

- Although the secondary DPOD node has a different IP address, all the DataPower appliances will still be able to access it since their internal host aliases pointing to DPOD will be replaced (step 2 above).
- As all DataPower appliances retain the same IP addresses - DPOD can continue to sample them.
- Although the secondary DPOD node has a different IP address, all users can access DPOD’s web console because its DNS name has been changed or it is behind an NLB (step 3 above).

> All Data from the originally Active DPOD will not be available!

In a "Return to Normal" scenario:

1. Right after re-launching the primary node, make a call to the "standbyToInactive" API (see DR REST API) to disable the standby node.
2. Call the "activeBackToActive" API (see DR REST API) to re-enable the primary node. This will point DPOD's log targets and host aliases on the monitored devices back to the primary DPOD node.
3. The customer's DR software should change the DNS name for the DPOD node's web console to reference an actual IP address or use an NLB in front of both DPOD web consoles.
4. During state transition of the Primary node from Active to Standby there might be some data loss.

SCENARIO D: LIMITED ACTIVE/ACTIVE – TWO SEPARATE DPOD INSTALLATIONS WITH NO SHARED STORAGE

Assumptions:

1. The customer has DataPower appliances deployed using either an Active/Passive, Active/Active or Active/Stand-by configuration. All DataPower appliances in any of these configurations have unique IP addresses.
2. Two DPOD nodes are installed (both are v1.0.5+), both running in Active state.
3. Both DPOD nodes must have **different** environment names. The environment name is set by the customer during DPOD software deployment, and is visible at the top navigation bar .
4. Both DPOD nodes are configured separately to monitor all DataPower Devices (active, standby and passive). Starting with DPOD v1.0.5 a new REST API may be utilized to add a new DataPower device to DPOD without using the UI (see Devices REST API). **As both nodes are up, no configuration replication can exist in this scenario.**
5. **As both nodes are up, no data replication can exist in this scenario.** The customer is expected to configure each DPOD node as a standalone deployment, including all system parameters, security groups / roles/ LDAP parameters / Certificates, custom reports and reports scheduling, custom alerts and alerts scheduling, maintenance plan and user preferences. DPOD is not performing any configuration synchronization.
6. Importantly, the customer must add DataPower instances to each installation to monitor all DataPower Devices (active, standby and passive). Starting with DPOD v1.0.5, a new REST API may be utilized to add a new DataPower device to DPOD without using the UI (see Devices REST API). The customer must add DataPower instances to the standby DPOD node and set the agents for each device from the Device Management page in the web console (or by using the Devices REST API). Setting up the devices in the standby DPOD node **will not** make any changes to the monitored DataPower devices (no log targets, host aliases or configuration changes will be made).
7. All DPOD network services (NTP, SMTP, LDAP etc.) have the same IP addresses.
8. The customer added DataPower devices to the standby DPOD node and set the agents for each device from the Device Management page in the web console (or by using the Devices REST API). **The customer is expected to replicate all configurations and definitions for each installation. DPOD replicates neither data nor configurations/definitions.**
9. **Important! -** Since the two installations are completely independent and no data is replicated - data inconsistency may follow, as one may capture information while the other is in Down state for maintenance or even started in different time. This might affect reports and alerts.
10. **Important! -** Each DPOD installation will create 2 log targets for each domain. If one DataPower is connected to 2 DPODs - then for each domain you will need 4 log targets. As DataPower have a limitation of ~1000 log targets starting FW 7.6, the customer must take care to not reach the log targets limit.
11. All logs and information will be sent twice over the network thus network bandwidth will be doubled !

During a disaster:

1. No action is required. The DataPower instance will push data to both instances.

DPOD will be available in the following way:

- The active node will continue to operate as it was operating before.
- All users can access DPOD’s web console because its DNS name has been changed or it is behind an NLB as it was accessible before the disaster.
- Note - Some Data from the originally Active DPOD will not be available

In a "Return to Normal" scenario:

1. No action is required. The DataPower instance will push data to both instance
2. The data gathered throughout the disaster period can not be synced back to the recovered node

Backups

To improve product recovery, an administrator should perform regular backups as described in the backup section.

Backups

There are several types of components in the DPOD appliance that should be backed up :

BACKUP SOFTWARE ,STATIC CONFIGURATION AND USER CONFIGURATION DATA (INTERNAL DB)

In order to backup DPOD's software, static configuration and user configuration data (internal DB) use the app_backup.sh script located in directory /app/scripts.

The scripts parameters :

Parameter	Purpose
-t, --backup-type	full (default) : application files and internal DB app : application files db : internal DB
-d, --backup-directory	The destination output backup directory . default is :/installs/system-backup/<backup type>-<current date and time> example for full backup : /installs/system-backup/full-backup-2017-11-02_18-52-08
-f, ---backup-file-name	The destination output backup file name. default is :<backup type>-<current date and time>.tar.gz example for full backup : full-backup-2017-11-02_18-52-08.tar.gz

Invoke the backup command

```
app_backup.sh
INFO : backup finished successfully. for more information see log file
/installs/system-backup/full-backup-2017-09-11_17-17-59/full-backup-2017
-09-11_17-17-59.log
```

The output backup directory will be the location of the backup log as printed in the backup status message (in the current example /installs/system-backup/full-backup-2017-09-11_17-17-59).

The free space required on the backup output directory could get up to 300MB (for DPOD version 1.0.6.0)

RESTORE SOFTWARE ,STATIC CONFIGURATION AND USER CONFIGURATION DATA (INTERNAL DB)

In order to restore DPOD's software, static configuration and user configuration data (internal DB) use the app_restore.sh script located in directory /app/scripts.

The scripts parameters :

Parameter	Purpose
-t, --restore-type	full : application files and internal DB app : application files db : internal DB
-d, --backup-directory	The restore source backup directory. in the example /installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56
-f, ---backup-file-name	The source backup file in the backup directory. in the example full-backup-2017-09-13_22-38-56.tar.gz

example for restoring internal DB :

```
app_restore.sh -t db -d
/installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56
-f full-backup-2017-09-13_22-38-56.tar.gz

stopping application ...
application stopped successfully.
starting restore process ...
restoring internal DB .....
system restore was successful
for more information see log file
/installs/system-backup/db-restore-2017-09-17_15-04-19.log
```

example for restoring software, static configuration :

```
app_restore.sh -t app -d
/installs/system-backup/system-migration/full-backup-2017-09-13_22-38-56
-f full-backup-2017-09-13_22-38-56.tar.gz

stopping application ...
application stopped successfully.
starting restore process ...
restoring system files ...
making sure files to restore exist in backup file
files to restore exist in backup file
system restore was successful
for more information see log file
/installs/system-backup/app-restore-2017-09-17_15-04-19.log
```

BACKUP THE STORE

> It is not recommended to backup the big data store using regular backup software due to its size . You should follow the instruction on how to create snapshot and export the data to HDFS.

AUTOMATIC BACKUP FOR MONITORED DEVICE BEFORE CRITICAL OPERATIONS

DPOD creates a backup of the monitored device or create a checkpoint before some Web Console operations that changes the monitored device.

The list of this operations appears in this table

This backups can be located at /data/ui/WdpBackups

> It is recommended that you should delete periodically these backups or move them to a secured location.

Backing up and Restoring DPODs IDG related configuration

There might be cases where DPOD users would like the ability to remove DPOD related configuration from a monitored device (IDG). One such case would be a requirement for temporary monitoring of a non-production device for product demonstration.

There are two methods available to remove DPOD related configuration from monitored IDG devices:

1. Manually, as describe in How to Uninstall DPOD from DataPower
2. Using the DPOD IDG configuration tool

The DPOD IDG configuration tool is a simple tool that enables users to backup the DPOD related configuration of IDG before starting to monitor the IDG using DPOD.

If required, the tool can also be used remove the DPOD configuration from IDG monitored device.

Backing up the IDG configuration

To perform an IDG configuration backup, use the app_idg_pre_conf_bck.sh script located in the /app/scripts directory.

The script will back up the following IDG objects configuration:

- XML management interface
- WS-M agent configuration (default domain and appliaction domains)
- Certificate monitor

The script parameters are :

Operation	Purpose
-i, --idg-ip	IDG xml management interface IP address or host name
-p, --idg-port	IDG xml management interface port
-u, --idg-user	IDG xml management interface username
-s, --idg-pass	IDG xml management interface user password

The script's backup directory and log file will be displayed in a message at the end of execution.

Example of the script execution :

```
app_idg_pre_conf_bck.sh -i 192.168.65.80 -p 5550 -u admin -s 123456
```

Removing DPOD configuration and restoring IDG objects based on the backup information

To remove the DPOD configuration from an IDG monitored device use the script app_idg_pre_conf_restore.sh located in the /app/scripts. directory.

> **If you did not run** app_idg_pre_conf_bck.sh before installing DPOD - you can still remove some of the configuration automatically by running it now, and letting it backup the current configuration.
> By doing so - the restore process will not revert the settings to the previous pre-DPOD state, but it will still automatically delete all DPOD's log targets and host aliases.

The script will restore the following IDG objects configuration based on the backup file :

- XML management interface
- WS-M agent configuration
- Certificate monitor

Furthermore, the script will remove the following DPOD related configuration:

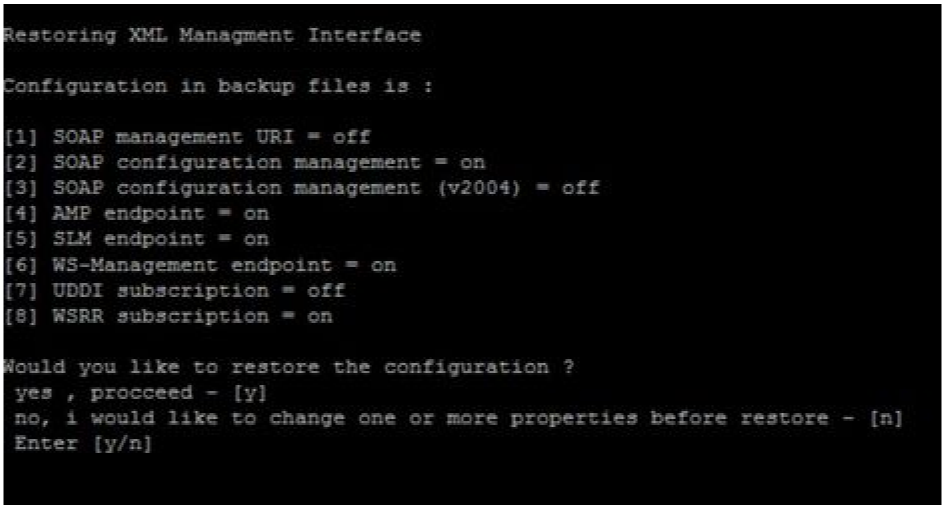
- DPOD related host aliases
- DPOD log targets
- DPOD log category
- Disable statistics
- Remove two XSLT files deployed by DPOD to store directory

The script parameters are :

Operation	Purpose
-i, --idg-ip	IDG xml management interface IP address or host name
-p, --idg-port	IDG xml management interface port
-u, --idg-user	IDG xml management interface username
-s, --idg-pass	IDG xml management interface user password
-d, --backup-dir	source backup directory If you do not remember the backup directory's name - search the path /installs/system-backup for a sub folder with the device's ip address

As the original backed up configuration might have changed between the period of the backup and the restore, the script displays the backup data and provides the user with an opportunity to change the configuration to restore.

This is an example of the XML management interface restore menu:



```
Restoring XML Managment Interface

Configuration in backup files is :

[1] SOAP management URI = off
[2] SOAP configuration management = on
[3] SOAP configuration management (v2004) = off
[4] AMP endpoint = on
[5] SLM endpoint = on
[6] WS-Management endpoint = on
[7] UDDI subscription = off
[8] WSRR subscription = on

Would you like to restore the configuration ?
 yes , procceed - [y]
 no, i would like to change one or more properties before restore - [n]
 Enter [y/n]
```

The script's log file will be displayed in a message at the end of execution.

If multiple DPODs are installed, and one of them still needs to monitor the DataPower device, the script may have removed objects that belong to it.
In this case, you will need to setup syslog again for the device and domains for this other DPOD, see Adding Monitored Devices for more information

The script does not remove the following objects, and the user will have to remove them manually, unless there is another DPOD monitoring the device:

Log Category - msc-mon
Host Alias - MonTier_LogTarget_Source
Only in API Connect domains - Log Category - api-mon

Disks' Replication Policy

REPLICATION POLICY

DPOD has 3 disks (DPOD Developer Edition is not supported for HA\DR):

- Disk 1 – Operating System,
- Disk 2 – Application & Configuration,
- Disk 3 – Data of all monitored Data Power's transaction and configuration.

1. For launching DPOD server in a replicated environment customer must replicate Disk1 and Disk 2 on a regular basis as they usually have a reasonable rate of changes.
2. Replicating Data Disk (Disk 3) can generate massive IOPS and bandwidth usage which can be a burden on the customer replication mechanism.
   In cases it is acceptable for customer to launch its passive server without the data, customer can follow this step to create a clean working data disk (disk 3):
   a. Customer must create a full back of disk 3 when all DPOD services are down.
   b. Customer must copy the backup of disk 3 to passive DPOD server storage and make sure it is attached to the passive DPOD server.
   c. Customer must start the passive DPOD server and verify that DPOD is fully started and operational.
   d. Customer should delete DPOD data (if exists) using the DPOD web console (Manage -> Internal Health -> Store)
   e. Customer can shut down the secondary DPOD and start the replication for DISK 1 and 2 only.
   f. After each DPOD upgrade it is recommended to rerun this procedure in case directory structure in Disk 3 changed.

Troubleshoot

This section contains a list of common issues you may encounter while using DPOD and how to troubleshoot them.

- Disable / Enable DPOD's log targets
- DPOD SSH Session Disconnects Often
- Payload Capture Settings and Authorization
- Payload capturing using WS-M does not provide results
- Running MustGather from CLI
- Unassigned Shards
- IDG WS-M payload capture support
- DPOD supported OS locale
- WS-M large payloads are not displayed
- Policy Variables Capture Settings and Authorization

Disable / Enable DPOD's log targets

You can disable or enable DPOD's log targets for the default domain, a specific domain or all domains.

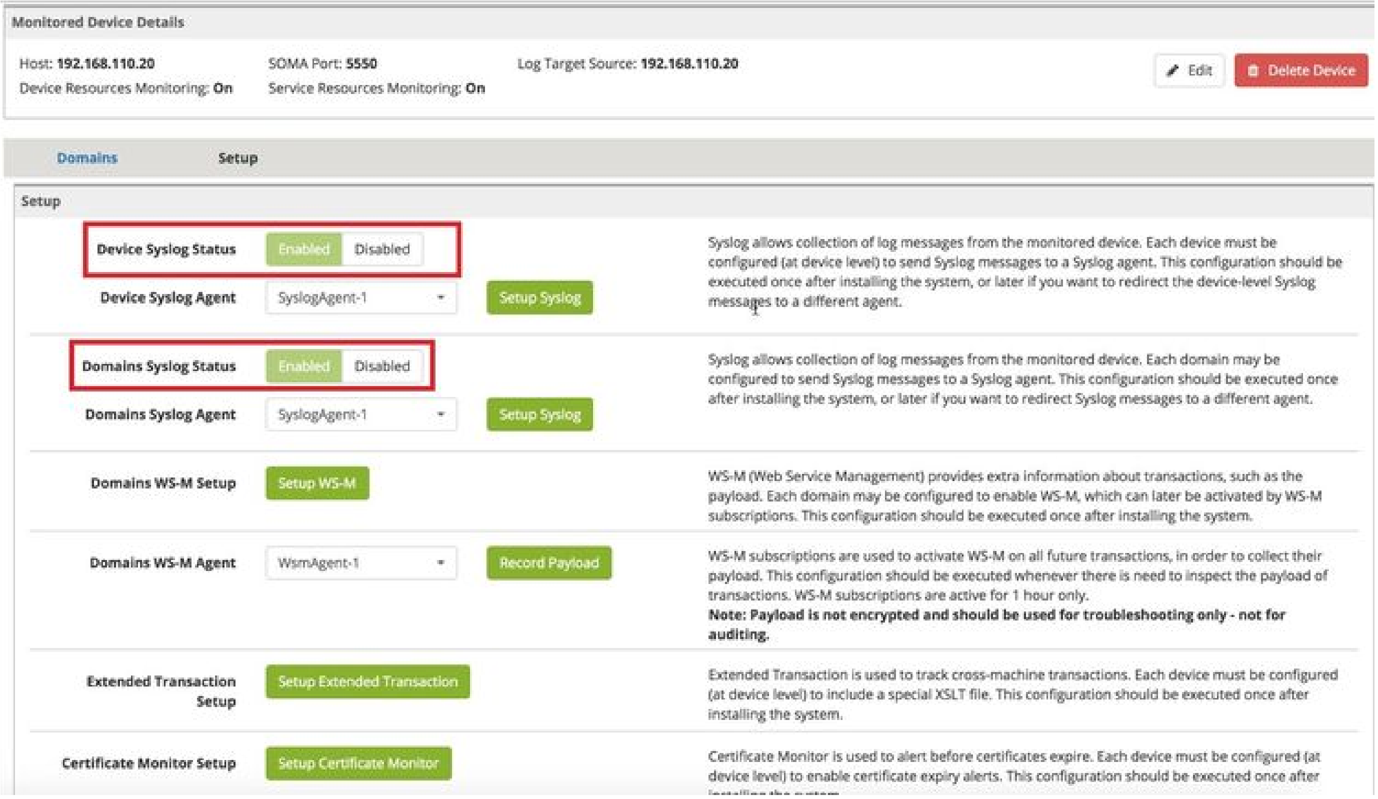
Disable/Enable on the Device Level

Go to the [**ManageManaged Devices]** menu

There are two relevant options:

The "**Device Syslog Status**" controls the log target on the default domain

The "**Domains Syslog Status**" controls all DPOD's log targets on all domains (except on the default domain)



Monitored Device Details

Host: **192.168.110.20** SOMA Port: **5550** Log Target Source: **192.168.110.20**

Device Resources Monitoring: **On** Service Resources Monitoring: **On**

Setup

Device Syslog Status

Device Syslog Agent SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each device must be configured (at device level) to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect the device-level Syslog messages to a different agent.

Domains Syslog Status

Domains Syslog Agent SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect Syslog messages to a different agent.

Domains WS-M Setup

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration should be executed once after installing the system.

Domains WS-M Agent WsmAgent-1

WS-M subscriptions are used to activate WS-M on all future transactions, in order to collect their payload. This configuration should be executed whenever there is need to inspect the payload of transactions. WS-M subscriptions are active for 1 hour only.
Note: Payload is not encrypted and should be used for troubleshooting only - not for auditing.

Extended Transaction Setup

Extended Transaction is used to track cross-machine transactions. Each device must be configured (at device level) to include a special XSLT file. This configuration should be executed once after installing the system.

Certificate Monitor Setup

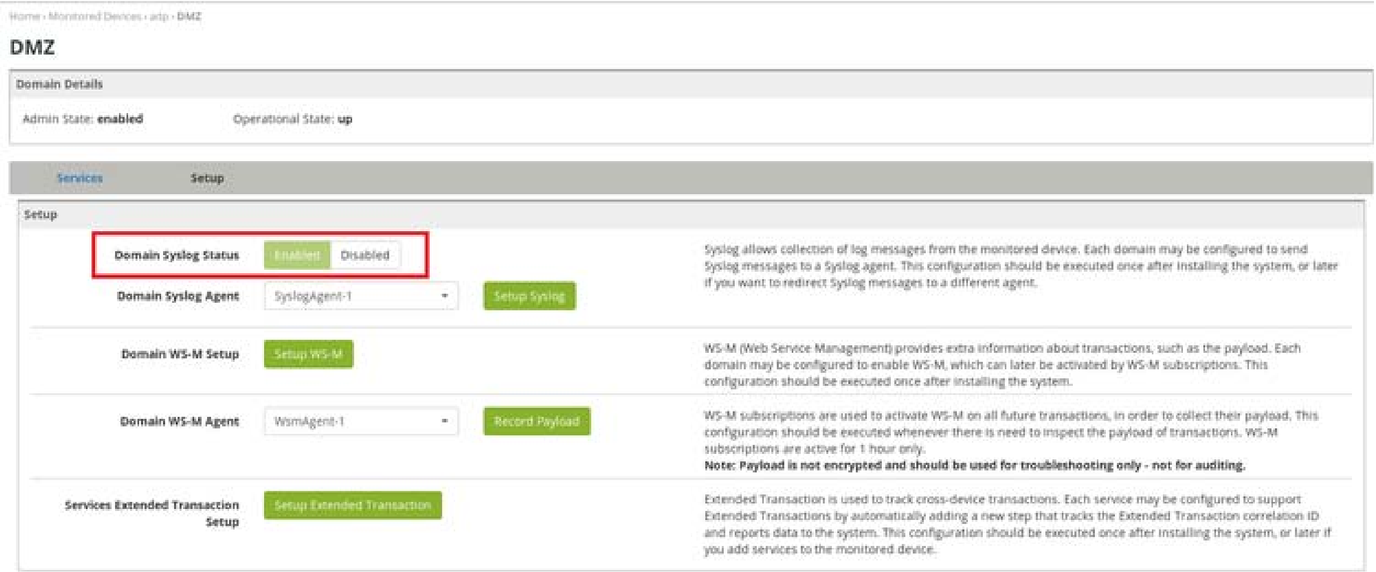
Certificate Monitor is used to alert before certificates expire. Each device must be configured (at device level) to enable certificate expiry alerts. This configuration should be executed once after

Disable/Enable a logtarget for a Specific Domain

You can disable/enable syslog for a specific domain -

Go to the [**ManageManaged Devices]** menu, choose a monitored device and click a domain from the list, click the "Setup" tab.

You can turn the logtarget on or off by clicking the appropriate "**Domain Syslog Status**" button



DMZ

Domain Details

Admin State: **enabled**

Operational State: **up**

Setup

Domain Syslog Status: Enabled

Domain Syslog Agent: SyslogAgent-1

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if you want to redirect Syslog messages to a different agent.

Domain WS-M Setup

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration should be executed once after installing the system.

Domain WS-M Agent: WsmAgent-1

WS-M subscriptions are used to activate WS-M on all future transactions, in order to collect their payload. This configuration should be executed whenever there is need to inspect the payload of transactions. WS-M subscriptions are active for 1 hour only.

Note: Payload is not encrypted and should be used for troubleshooting only - not for auditing.

Services Extended Transaction Setup

Extended Transaction is used to track cross-device transactions. Each service may be configured to support Extended Transactions by automatically adding a new step that tracks the Extended Transaction correlation ID and reports data to the system. This configuration should be executed once after installing the system, or later if you add services to the monitored device.

DPOD SSH Session Disconnects Often

As part of the appliance hardening, a short timeout value (300 seconds) is set for the SSH session.

If you need to perform long-running system activities, please issue the following commands:

disable ssh disconnect

```
sed -i '/^.*ClientAliveInterval.*$/d' /etc/ssh/sshd_config
sed -i '/^.*ClientAliveCountMax.*$/d' /etc/ssh/sshd_config
service sshd restart
```

Once your long running activity has completed, issue the following commands to reinstate the short timeout settings.

```
sed -i 's/^.*ClientAliveInterval.*$/#ClientAliveInterval 300/'
/etc/ssh/sshd_config
sed -i 's/^.*ClientAliveCountMax.*$/#ClientAliveCountMax 0/'
/etc/ssh/sshd_config
service sshd restart
```

Payload Capture Settings and Authorization

DPOD lets users create new WS-M subscriptions from the Payload Capture page.

AUTHORIZATION

This page will be accessible for the following users:

- Admins (users with the OpDashAdminRole Role)
- Users that has a custom role with both "Allow Payload" and "Manage Payload Capture" set to Yes

> For users that has multiple roles - the user will NOT have access if one of the roles has "allow Payload" or "Mange Payload Capture" set to No, even if another role sets them to Yes

Please note that the payload capture screen takes allowed/denied devices and domain into consideration, users that does not have access to a certain domain, will not be able to view its subscriptions or create new subscriptions for this domain.

SUBSCRIPTION DURATION SETTINGS

For Admin users - You can control the maximum duration in minutes of WS-M subscriptions by changing the option "**Max Number of Minutes for WS-M Subscription Created by an Admin**" from the system parameter page

For Non-Admin users - You can control the maximum duration in minutes of WS-M subscriptions by changing the option "**Max Number of Minutes for WS-M Subscription Created by non-Admin**" from the system parameter page

WS-M AGENT SELECTION

The DPOD agent that will be used is setup in the Device Management page

AUTOMATIC DELETION FROM STORE

Payloads can be automatically deleted from store after one day or one week - see "Time to Keep WS-M Payloads" in system parameters , if this value is not set, payloads will be deleted when the store fills up (earliest ones will be deleted first), the exact time depends on your store allocation size

Payload capturing using WS-M does not provide results

There are several reasons why payloads may not show in DPOD:

1. Payloads capture is not supported
2. Payloads are not being sent
3. Payloads capture has errors, or filtered out in DPOD
4. Payloads are fully collected in DPOD, but are still not displayed

Perform the following checks to find the cause in your case:

PAYLOADS CAPTURE IS NOT SUPPORTED

Payload capture is only supported for:

1) WS Proxy objects in any firware 6.1.X and above

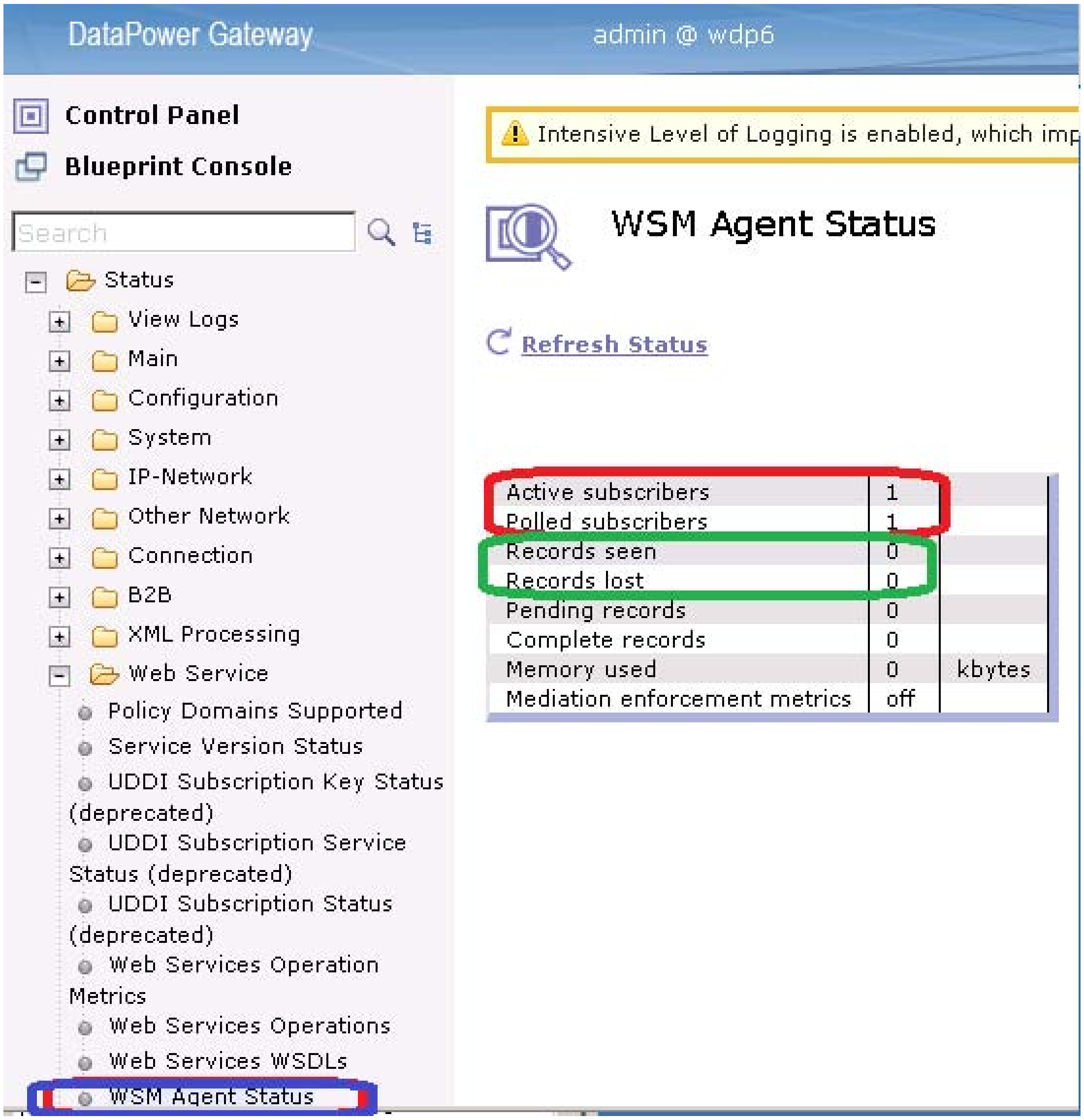
2) MPGW objects from IDG firmware 7.5.2 and DPOD 1.0.2 (text payloads only)

To see payloads on a non-supported object type and/or versions please upgrade or submit an RFE.

PAYLOADS ARE NOT BEING SENT

Perform the following to verify that payload capture is enabled:

- Verify WS-M capturing is enabled: by following the directions under WS-M setup for device and WS-M Subscriptions for All Domains (Optional) as they appear in Adding Monitored Devices
- Verify on your IDG that the subscriptions are created: In the expected domain navigate to Status Web Service WSM Agent Status (see blue hilight in the screenshot below). You should see 1 Active subscriber of polled type (see red highlight).
  If payloads were captured then they will be reported as Records seen.
  Additional statistic data can be seen on WSM:

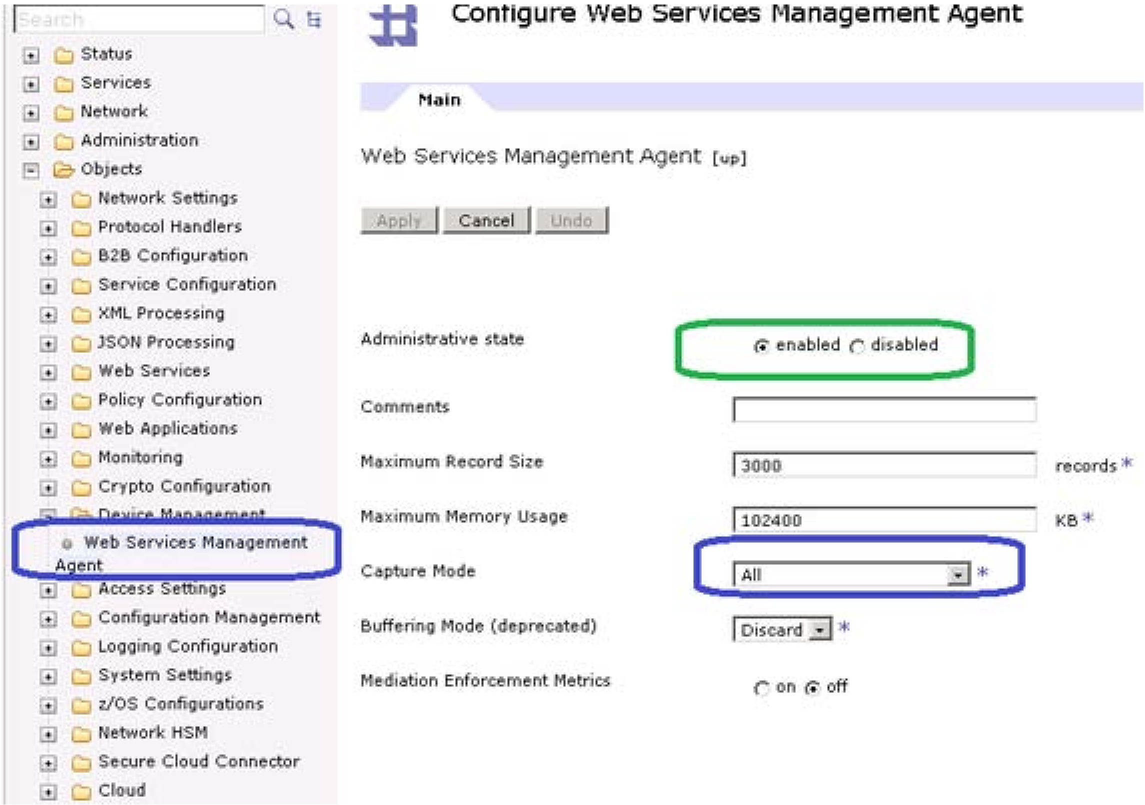


Intensive Level of Logging is enabled, which imp

WSM Agent Status

Active subscribers	1	
Polled subscribers	1	
Records seen	0	
Records lost	0	
Pending records	0	
Complete records	0	
Memory used	0	kbytes
Mediation enforcement metrics	off	

- If Records Seen value is 0, this may mean you do not have running transactions
- If Active Subscribers value is 1 and the value of Polled Subscribers is 0 - ensure you have followed the next step:
- Check that the WS-M Agent in IDG is configured correctly:



Configure Web Services Management Agent

Web Services Management Agent [up]

Administrative state ● enabled ○ disabled

Comments

Maximum Record Size 3000 records *

Maximum Memory Usage 102400 KB *

Capture Mode All *

Buffering Mode (deprecated) Discard *

Mediation Enforcement Metrics ○ on ● off

- DPOD expects the WS-M Agent to be **enabled** and Capture Mode to be set to **All**
- If your WS-M agent is enabled in IDG, you can create a subscription on DPOD by performing step WS-M Subscriptions for All Domains (Optional) on Adding Monitored Devices. If the Records Seen counter increases by any running transaction - then the payload should arrive at the DPOD WS-M Agent

PAYLOADS ARE SENT BUT FILTERED OUT

If you know that payloads are sent to the DPOD WS-M agent but still can not see them, follow the steps below to ensure they arrive and are being processed.

- Verify the DPOD WS-M agent is up and running - Check System Services Status with the CLI.
- Verify that the DPOD WS-M agent status is green on Check System Status Using the Web Console. This means that the keep alive message are processed.
- Inspect the WS-M logs for any exceptions. Logs may be accessed using Telnet, at the following path: /logs/wsmAgents/<Agent-name>/agent-flume_<Agent-name>.log.
  Normal WS-M log records should show:

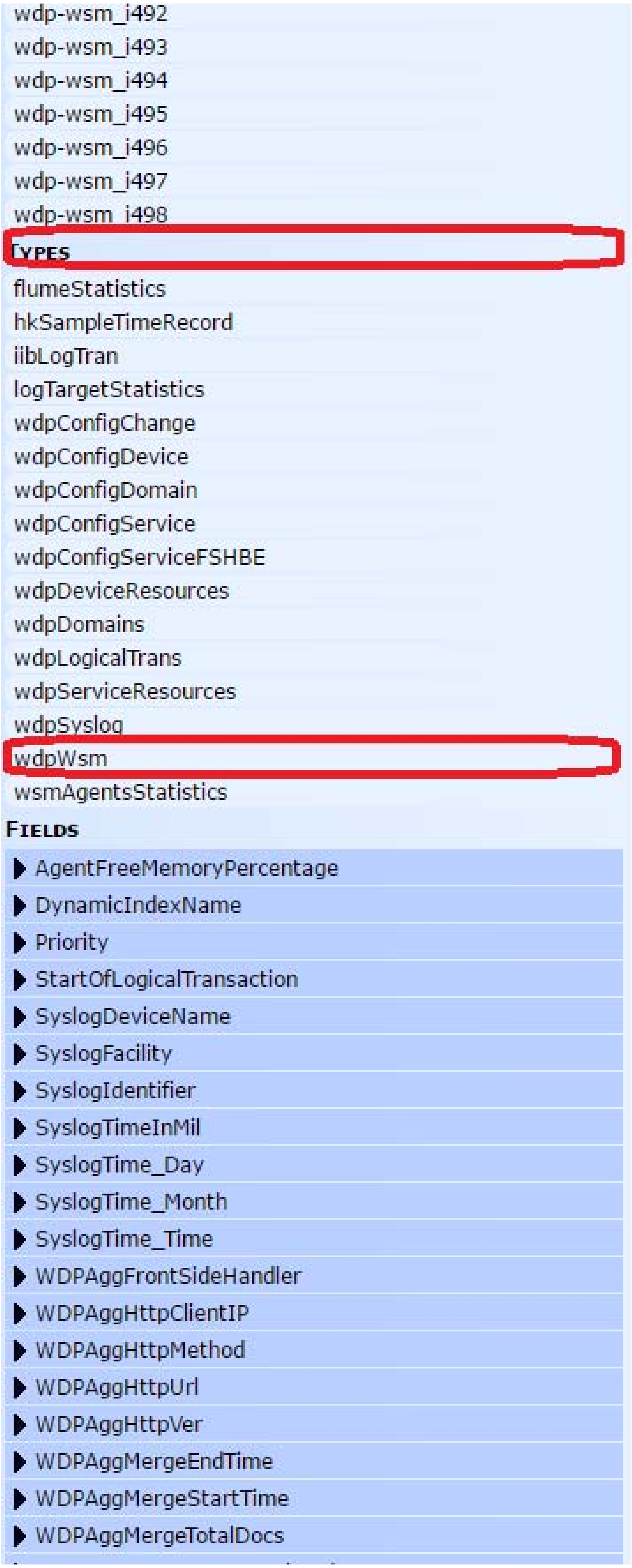
```
11/10/XXXX 08:26:03,477- INFO o.m.a.f.h.NHttpFileServer [I/O-dispatch-2] wsmHttpSource1 Incoming
entity content (bytes): 2908.   an actual payload arrived
11/10/XXXX 08:26:10,166- INFO o.m.a.f.h.NHttpFileServer [I/O-dispatch-3] wsmHttpSource1 Incoming
entity content (bytes): 2220.   size 2220 means usually keep alive message
```

- To find exceptions in your logs, enter the search term ' ERROR ' (leading and trailing space). Contact support with any exception found.
- In some cases DPOD may filter messages out because of their size. Please see the following technote: WS-M large payloads are not displayed

PAYLOADS ARE FULLY COLLECTED IN DPOD, BUT ARE STILL NOT DISPLAYED

This is usually caused because of bad synchronization of time and timezones between IDG and DPOD.

- You should see your transaction in DPOD (without payload) under Investigate Transaction.
- You will be able too see your payload if you go to DPOD Web console Manage Internal Health Store and click the **ES-Head** button at top right corner.
- Once inside **ES-Head** click on the "Browser" tab and scroll down to find **wdpWsm** under the **Types** header on the left hand side. Click **wdpWsm.**



wdp-wsm_i492
wdp-wsm_i493
wdp-wsm_i494
wdp-wsm_i495
wdp-wsm_i496
wdp-wsm_i497
wdp-wsm_i498

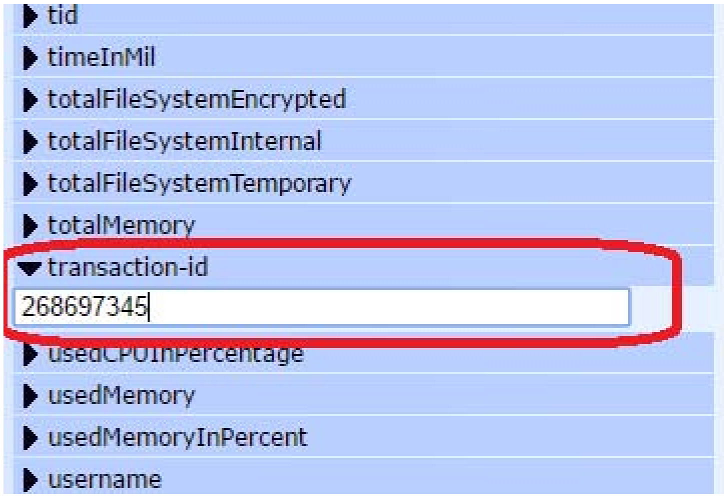
TYPES

flumeStatistics
hkSampleTimeRecord
iibLogTran
logTargetStatistics
wdpConfigChange
wdpConfigDevice
wdpConfigDomain
wdpConfigService
wdpConfigServiceFSHBE
wdpDeviceResources
wdpDomains
wdpLogicalTrans
wdpServiceResources
wdpSyslog
wdpWsm
wsmAgentsStatistics

FIELDS

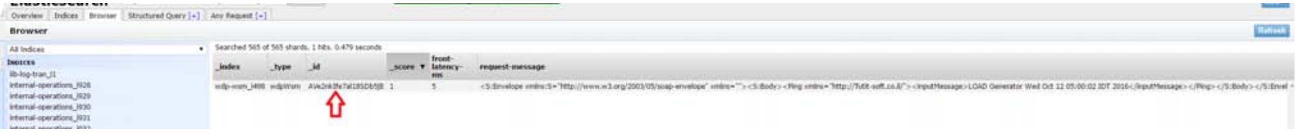
- AgentFreeMemoryPercentage
- DynamicIndexName
- Priority
- StartOfLogicalTransaction
- SyslogDeviceName
- SyslogFacility
- SyslogIdentifier
- SyslogTimeInMil
- SyslogTime_Day
- SyslogTime_Month
- SyslogTime_Time
- WDPAggFrontSideHandler
- WDPAggHttpClientIP
- WDPAggHttpMethod
- WDPAggHttpUrl
- WDPAggHttpVer
- WDPAggMergeEndTime
- WDPAggMergeStartTime
- WDPAggMergeTotalDocs

- Find **transaction-id** under **Fields** and a list of fields and enter the transaction id you are interested in.



- tid
- timeInMil
- totalFileSystemEncrypted
- totalFileSystemInternal
- totalFileSystemTemporary
- totalMemory
- transaction-id: 268697345
- usedCPUInPercentage
- usedMemory
- usedMemoryInPercent
- username

- Scroll back up to the top. Your payload now appears. click on it to view a JSON payload.

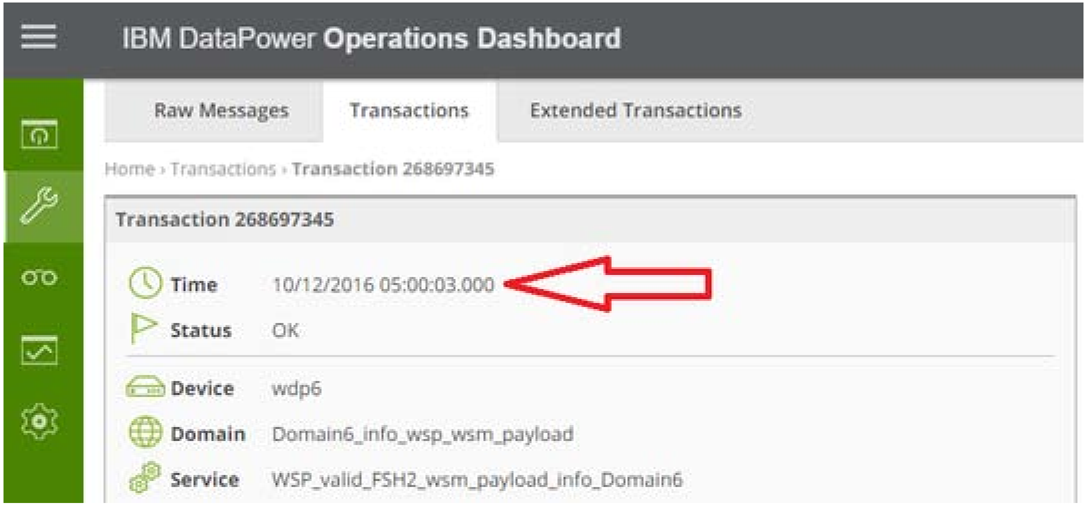


Searched 565 of 565 shards. 1 hits. 0.479 seconds

_index	_type	_id	_score ▼	front-latency-ms	request-message
wdp-wsm_J408	wdpWsm	AVe2nk8fe7al18SDb5j8	1	5	<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope" xmlns=""><S:Body><Ping xmlns="http://Tu68-soft.co.il/"><inputMessage>LOAD Generator Wed Oct 12 05:00:02 IDT 2016</inputMessage></Ping></S:Body></S:Envel

- In the JSON locate the start-time field.
`"start-time": "1476237603"`

  this is an epoch time. Use an online epoch converter to find the time of payload. Compare this to the transaction time as displayed under Investigate:



IBM DataPower Operations Dashboard
Raw Messages
Transactions
Extended Transactions
Home › Transactions › Transaction 268697345

Transaction 268697345

Time 10/12/2016 05:00:03.000
Status OK
Device wdp6
Domain Domain6_info_wsp_wsm_payload
Service WSP_valid_FSH2_wsm_payload_info_Domain6

- These should be the same (or within 5 minutes). If they are not - you need to adjust time and timezones in both IDG and DPOD. As best practice, you should configure both IDG and DPOD to the same NTP source.

Running MustGather from CLI

The MustGather utility will collect needed information for problem determination.

You have 2 options to run the tool :

- You can run Option 7 from CLI Main Admin Menu
  OR
- You can run the MustGather using the command line :

```
cd /app/scripts
must_gather.sh full
```

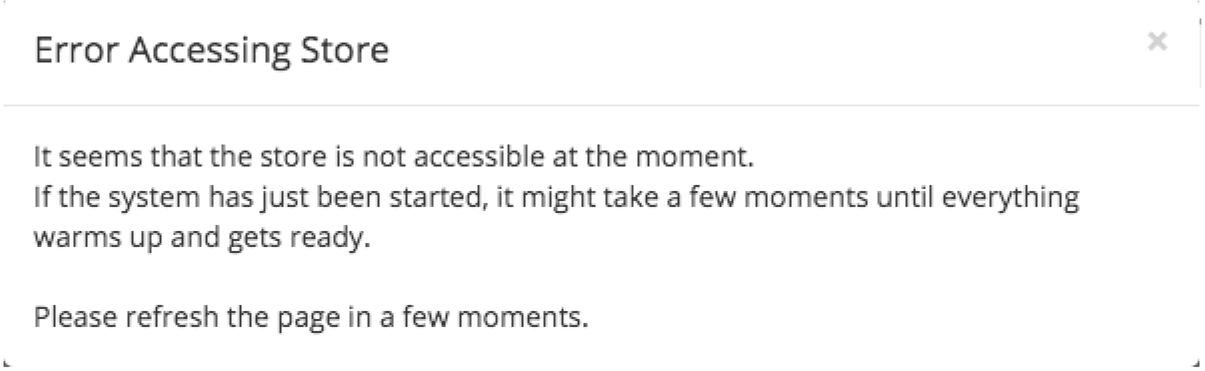
The command will generate compressed archive file containing information and log in /tmp directory.

example : /tmp/all_created_tar_export_2016-05-01_16-00-51.tgz

Unassigned Shards

Reallocating unassigned shards might solve the following situations:

1. An "Error Accessing Store" dialog is displayed after signing in to the system:

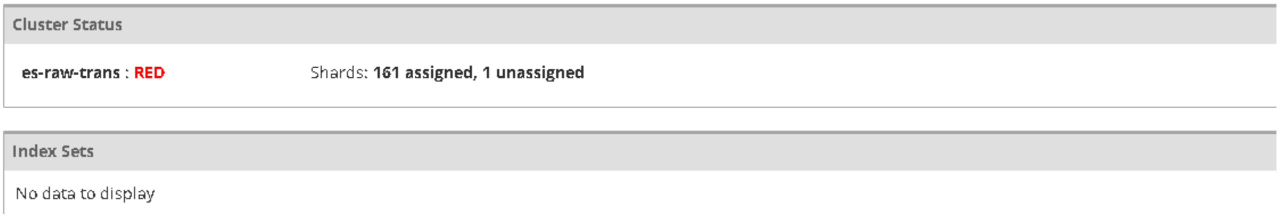


Error Accessing Store

It seems that the store is not accessible at the moment.
If the system has just been started, it might take a few moments until everything warms up and gets ready.

Please refresh the page in a few moments.

2. In the Store page, the status of the cluster is RED with unassigned shards:



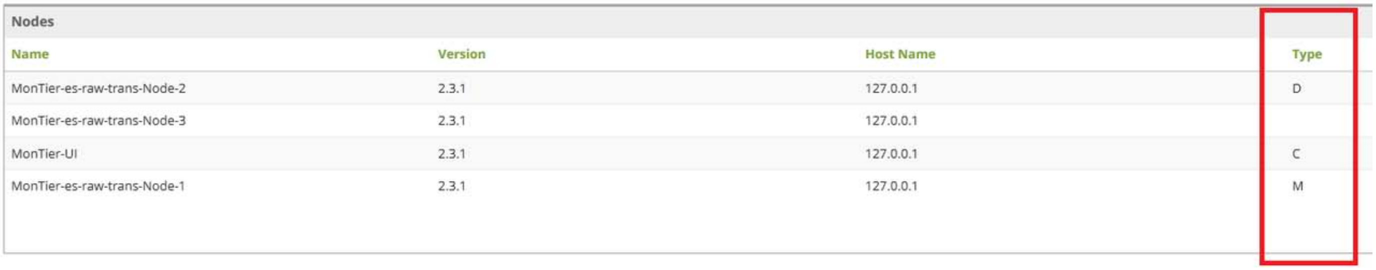
Cluster Status

es-raw-trans : RED Shards: **161 assigned, 1 unassigned**

Index Sets

No data to display

The store is divided into nodes (some used to keep data, others can handle communications or manage the cluster). The type of each node can be found in the Nodes table under "Type" column, marked in red in the following screenshot:



Nodes

Name	Version	Host Name	Type
MonTier-es-raw-trans-Node-2	2.3.1	127.0.0.1	D
MonTier-es-raw-trans-Node-3	2.3.1	127.0.0.1	
MonTier-UI	2.3.1	127.0.0.1	C
MonTier-es-raw-trans-Node-1	2.3.1	127.0.0.1	M

Shards need to be allocated/assigned to data nodes in order to be able to be populated with data. If shards are unassigned to a data node then no data can flow to the system.

This situation is usually caused by unexpected recovery of the cluster, where automatic assignment of shards was not applicable at the time of recovery for unknown reason.

To fix the issue, you may execute the following script: /app/scripts/realloc_shards.sh <Node Name>

- The <Node Name> parameter should be the name of the data node (a node of type "D" in the nodes table)

The script scans all shards and reallocates unassigned shards to the data node provided.

In the example above, the script should be run as follows:

```
/app/scripts/realloc_shards.sh MonTier-es-raw-trans-Node-2
```

This operation may take a while, depending on your installation and the amount of data. Refreshing the screen in "head" application (available from Store page) will show up-to-date state of the assigned and unassigned shards.

In cell environments, unassigned shards can only reallocate to a Store node from the same cell member or cell manager.
i.e. if there are unassigned shards from index of node N002, they can be reallocated to Store node named MonTier-es-raw-trans-N002-Node-X.

Below is an example of a successful execution:

```
Reallocation node: MonTier-es-raw-trans-Node-2
Testing index 0;wdp-wsm_i2
About to reallocate. index=wdp-wsm_i2, shard=0,
node=MonTier-es-raw-trans-Node-2
Reallocation http response status is: 200,
output={"acknowledged":true,"state":{"version":
Testing index 1;wdp-syslog-sys-auth_i1
About to reallocate. index=wdp-syslog-sys-auth_i1, shard=1,
node=MonTier-es-raw-trans-Node-2
Reallocation http response status is: 200,
output={"acknowledged":true,"state":{"version":
Testing index 2;system-health_i1
About to reallocate. index=system-health_i1, shard=2,
node=MonTier-es-raw-trans-Node-2
Reallocation http response status is: 200,
output={"acknowledged":true,"state":{"version":
Testing index 0;system-health_i1
About to reallocate. index=system-health_i1, shard=0,
node=MonTier-es-raw-trans-Node-2
Reallocation http response status is: 200,
output={"acknowledged":true,"state":{"version":
...
```

Below is an example of a unsuccessful execution:

```
Reallocation node: MonTier-es-raw-trans-Node-5
Testing index 0;wdp-syslog-sys-auth_i6
About to reallocate. index=wdp-syslog-sys-auth_i6, shard=0,
node=MonTier-es-raw-trans-Node-5
Reallocation http response status is: 400,
output={"error":{"root_cause":[{"type":"remote_
Testing index 0;wdp-syslog-sys-auth_i3
About to reallocate. index=wdp-syslog-sys-auth_i3, shard=0,
node=MonTier-es-raw-trans-Node-5
Reallocation http response status is: 400,
output={"error":{"root_cause":[{"type":"remote_
Testing index 1;logical-tran-full_i1
About to reallocate. index=logical-tran-full_i1, shard=1,
node=MonTier-es-raw-trans-Node-5
Reallocation http response status is: 400,
output={"error":{"root_cause":[{"type":"remote_
Testing index 1;wdp-config-service_i1
About to reallocate. index=wdp-config-service_i1, shard=1,
node=MonTier-es-raw-trans-Node-5
Reallocation http response status is: 400,
output={"error":{"root_cause":[{"type":"remote_
...
```

IDG WS-M payload capture support

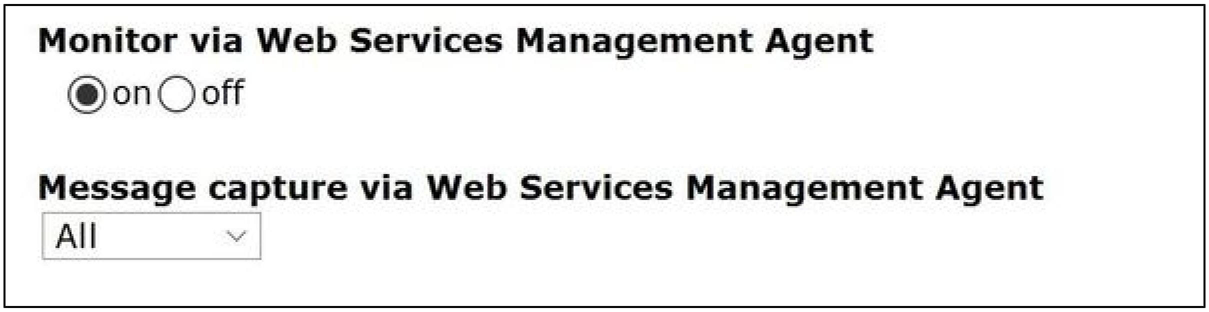
Web Services Management (WS-M) payload capture is supported by IDG for the following services:

1. Web Service Proxy starting firmware version 6.1.x .
2. Multi-Protocol Gateway starting firmware version 7.5.2.1 and DPOD version 1.0.2 for payload formats XML and JSON.

In order for the IDG to capture payload via WS-M the following IDG configuration is needed:

1. Web Service Proxy – Can be fully configured via DPOD since there is no need to change service configuration.
2. Multi-Protocol Gateway – The following configuration needs to be done in the service configuration:

- Enable the WS-M agent configuration in the Multi-Protocol Gateway service
    - Enter the service -> advanced tab -> turn “Monitor via Web Services Management Agent” to “on”.
    - Choose “All” in the “Message capture via Web Services Management Agent” filed.



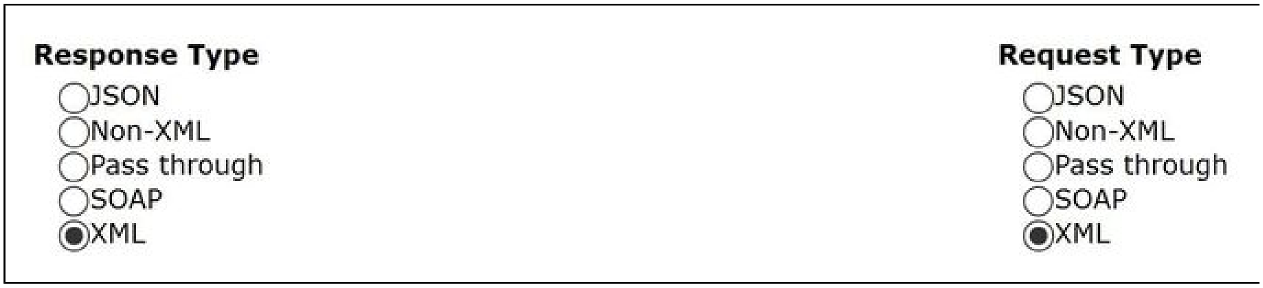
Monitor via Web Services Management Agent

● on ○ off

Message capture via Web Services Management Agent

All

- Enable XML / JSON parsing
  The WS-M agent capture only parsed XML and JSON formats. In order for the service to parse the payload the following service configuration are needed.
    - **Option one** - Change the “Request Type” and the “Response Type” to XML, JSON or SOAP.
      Note – If only one of the service direction (request or response) is configured with the supported payload formats then only payload from that direction will be captured.



Response Type

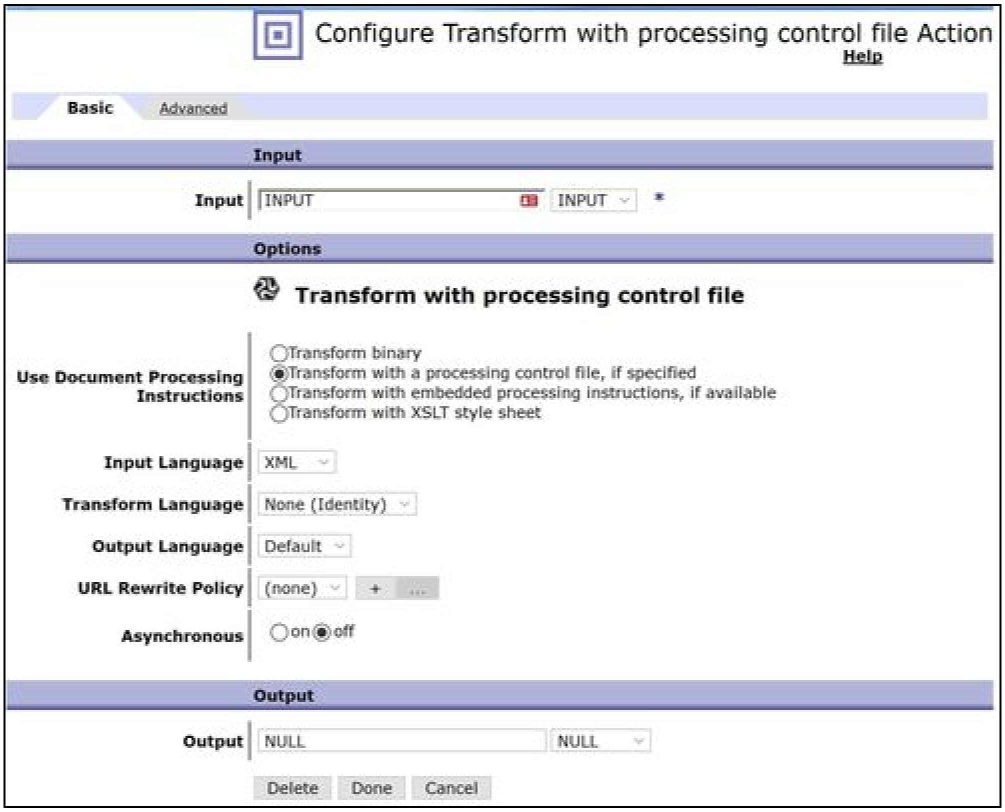
○ JSON
○ Non-XML
○ Pass through
○ SOAP
● XML

Request Type

○ JSON
○ Non-XML
○ Pass through
○ SOAP
● XML

-
    - **Option two** – If you must configure the request and response type as “non-xml” you can add “transform” action to the processing policy that will cause payload parse.
        - In every processing rule add “Transform with processing control file” action.
        - Choose the input=INPUT, output=NULL, “Input language”=XML or JSON according to the service design.

Due to IDG limitation the client request may not be captured.



Configure Transform with processing control file Action

Input

Input: INPUT | INPUT *

Options

Transform with processing control file

Use Document Processing Instructions:
○ Transform binary
● Transform with a processing control file, if specified
○ Transform with embedded processing instructions, if available
○ Transform with XSLT style sheet

Input Language: XML

Transform Language: None (Identity)

Output Language: Default

URL Rewrite Policy: (none)

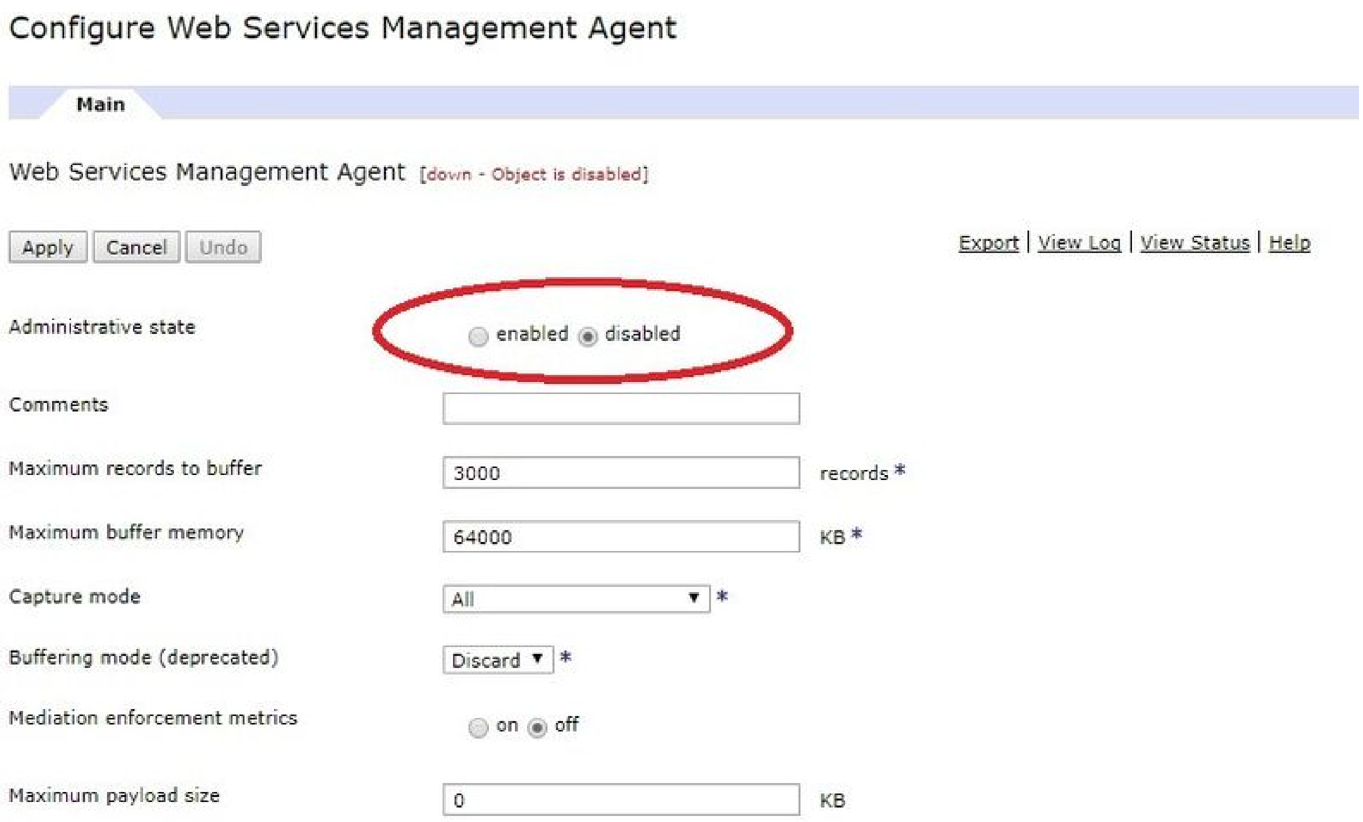
Asynchronous: ○ on ● off

Output

Output: NULL | NULL

WEB SERVICES MANAGEMENT AGENT

For each domain you would like to capture payload, you will need to manually enable the web services management agent (if it's disabled)



Configure Web Services Management Agent

Web Services Management Agent [down - Object is disabled]

Administrative state ○ enabled ● disabled

Comments

Maximum records to buffer 3000 records *

Maximum buffer memory 64000 KB *

Capture mode All *

Buffering mode (deprecated) Discard *

Mediation enforcement metrics ○ on ● off

Maximum payload size 0 KB

However, if you will try to configure WS-M subscriptions to all domain from DPOD and at least one of the domains is in disabled state, than you will get an error message ".. Subscription Manager reached maximum number od subscriptions". In that case you should configure each domain speratley or enable Web Service Management Agent for all domains.

DPOD supported OS locale

The only supported operating system locale definition for DPOD is **en_US.UTF-8**.

For appliance installation, this locale is configured automatically.

Non-Appliance installation should be configured to the supported locale using the following steps.

IDENTIFYING THE CURRENT LOCALE

login to the Non-Appliance server using SSH and run the following command:

```
localectl status
```

The command output should be:

```
System Locale: LANG=en_US.UTF-8
       VC Keymap: us
      X11 Layout: us
```

SETTING CORRECT LOCALE

If the Non-Appliance server is configured with a different locale - configure the supported locale:

1. Set the new locale using the following command:

   ```
   localectl set-locale LANG=en_US.UTF-8
   ```

2. Use the same steps as before to identify the current locale:

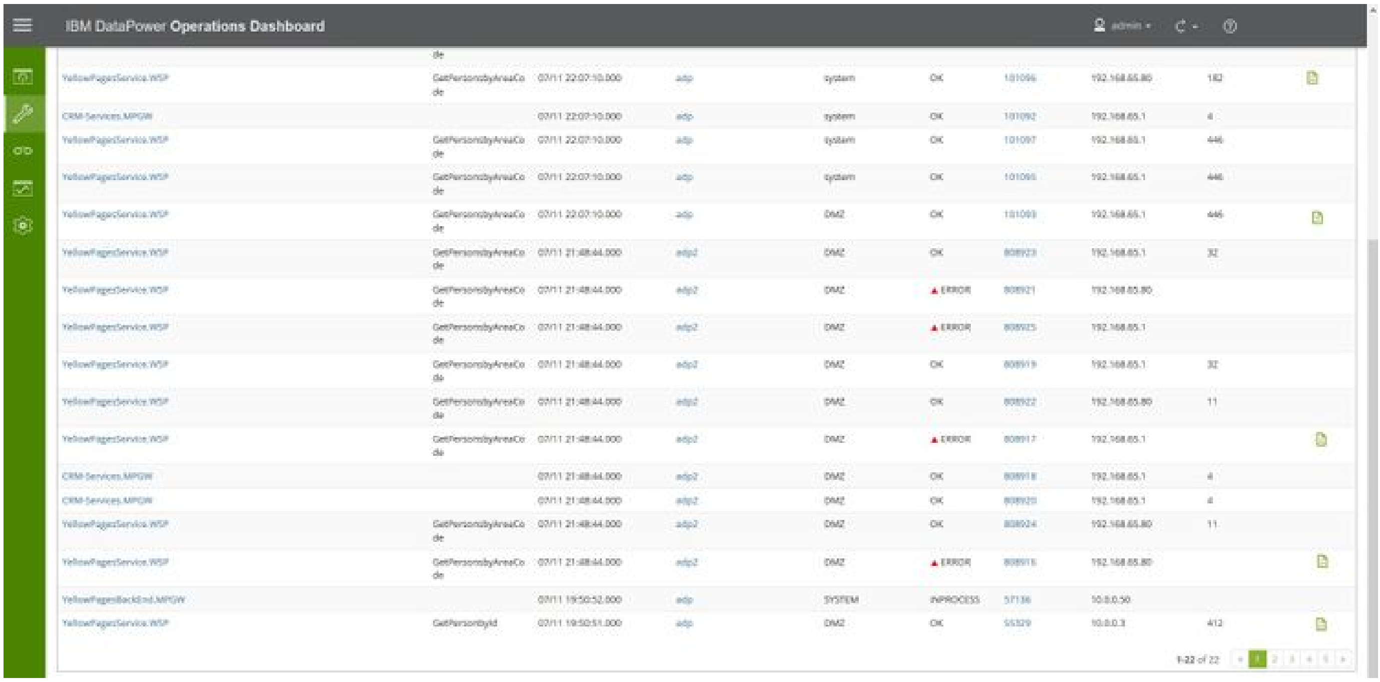
   ```
   localectl status
   System Locale: LANG=en_US.UTF-8
          VC Keymap: us
         X11 Layout: us
   ```

3. Restart the server

WS-M large payloads are not displayed

Symptoms

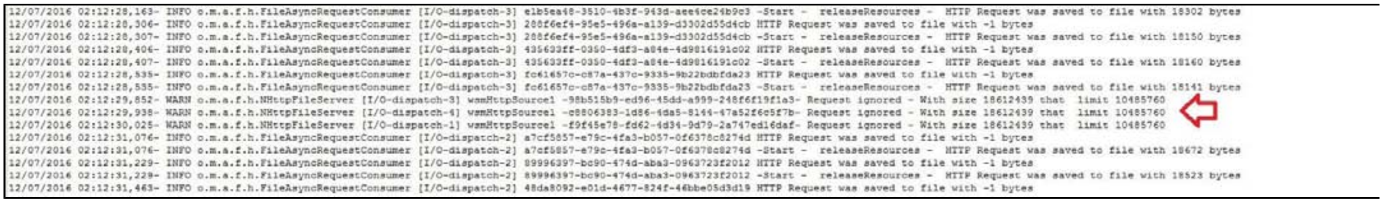
Some transactions are not showing WS-M Payloads, even though WS-M subscription was requested for them.



	de								
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 22:07:10.000	adp	system	OK	101096	192.168.65.80	182	🗎
CRM-Services.MPGW		07/11 22:07:10.000	adp	system	OK	101092	192.168.65.1	4	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 22:07:10.000	adp	system	OK	101097	192.168.65.1	446	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 22:07:10.000	adp	system	OK	101095	192.168.65.1	446	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 22:07:10.000	adp	DMZ	OK	101093	192.168.65.1	446	🗎
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	OK	808923	192.168.65.1	32	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	▲ ERROR	808921	192.168.65.80		
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	▲ ERROR	808925	192.168.65.1		
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	OK	808919	192.168.65.1	32	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	OK	808922	192.168.65.80	11	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	▲ ERROR	808917	192.168.65.1		🗎
CRM-Services.MPGW		07/11 21:48:44.000	adp2	DMZ	OK	808918	192.168.65.1	4	
CRM-Services.MPGW		07/11 21:48:44.000	adp2	DMZ	OK	808920	192.168.65.1	4	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	OK	808924	192.168.65.80	11	
YellowPagesService.WSP	GetPersonsbyAreaCode	07/11 21:48:44.000	adp2	DMZ	▲ ERROR	808916	192.168.65.80		🗎
YellowPagesBackEnd.MPGW		07/11 19:50:52.000	adp	SYSTEM	INPROCESS	57136	10.0.0.50		
YellowPagesService.WSP	GetPersonbyId	07/11 19:50:51.000	adp	DMZ	OK	55329	10.0.0.3	412	🗎

In /logs/wsmAgents/agent-flume_MonTier-WsmAgent-**X**.log (where **X** is the number of the DPOD WSM agent you use), you will see the following message(s):

12/07/2016 02:12:29,852- WARN o.m.a.f.h.NHttpFileServer [I/O-dispatch-3] wsmHttpSource1 -98b515b9-ed96-45dd-a999-248f6f19f1a3- Request ignored - With size 18615431 that limit 10485760



```
12/07/2016 02:12:28,163- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] e1b5ea48-3510-4b3f-943d-aee4ce24b9c3 -Start -  releaseResources -  HTTP Request was saved to file with 18302 bytes
12/07/2016 02:12:28,306- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] 288f6ef4-95e5-496a-a139-d3302d55d4cb HTTP Request was saved to file with -1 bytes
12/07/2016 02:12:28,307- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] 288f6ef4-95e5-496a-a139-d3302d55d4cb -Start -  releaseResources -  HTTP Request was saved to file with 18150 bytes
12/07/2016 02:12:28,406- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] 435633ff-0350-4df3-a84e-4d9816191c02 HTTP Request was saved to file with -1 bytes
12/07/2016 02:12:28,407- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] 435633ff-0350-4df3-a84e-4d9816191c02 -Start -  releaseResources -  HTTP Request was saved to file with 18160 bytes
12/07/2016 02:12:28,535- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] fc61657c-c87a-437c-9335-9b22bdbfda23 HTTP Request was saved to file with -1 bytes
12/07/2016 02:12:28,535- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-3] fc61657c-c87a-437c-9335-9b22bdbfda23 -Start -  releaseResources -  HTTP Request was saved to file with 18141 bytes
12/07/2016 02:12:29,852- WARN o.m.a.f.h.NHttpFileServer [I/O-dispatch-3] wsmHttpSource1 -98b515b9-ed96-45dd-a999-248f6f19f1a3- Request ignored - With size 18612439 that  limit 10485760
12/07/2016 02:12:29,938- WARN o.m.a.f.h.NHttpFileServer [I/O-dispatch-4] wsmHttpSource1 -c8806383-1d86-4da5-8144-47a52f6c5f7b- Request ignored - With size 18612439 that  limit 10485760
12/07/2016 02:12:30,025- WARN o.m.a.f.h.NHttpFileServer [I/O-dispatch-1] wsmHttpSource1 -f9f45e78-fd62-4d34-9d79-2a747ed16daf- Request ignored - With size 18612439 that  limit 10485760
12/07/2016 02:12:31,076- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-2] a7cf5857-e79c-4fa3-b057-0f6378c8274d HTTP Request was saved to file with -1 bytes
12/07/2016 02:12:31,076- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-2] a7cf5857-e79c-4fa3-b057-0f6378c8274d -Start -  releaseResources -  HTTP Request was saved to file with 18672 bytes
12/07/2016 02:12:31,229- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-2] 89996397-bc90-474d-aba3-0963723f2012 HTTP Request was saved to file with -1 bytes
12/07/2016 02:12:31,229- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-2] 89996397-bc90-474d-aba3-0963723f2012 -Start -  releaseResources -  HTTP Request was saved to file with 18523 bytes
12/07/2016 02:12:31,463- INFO o.m.a.f.h.FileAsyncRequestConsumer [I/O-dispatch-2] 48da8092-e01d-4677-824f-46bbe05d3d19 HTTP Request was saved to file with -1 bytes
```

Overview

Each WS-M event contains 4 payloads: Front-End request, Back-End request, Back-End response and Front-End response, the size of a single event equals to the size of all 4 payloads combined.
The DataPower batches several transactions (WS-M events) together before sending them to DPOD as a single request. The default setting is grouping 20 events together.

DPOD's WS-M Agent sets a size limit for incoming request. The default limit is 10mb, meaning DPOD will drop any requests that are larger than 10mb

Using those defaults may cause DPOD to drop requests. Consider the case where transaction payload size is 1mb (300kb back-end and front-end requests, and 200kb back-end and front-end responses). With the defaults in place, DataPower groups 20 transactions before sending them to DPOD. This will generate a total request size will of 20mb. DPOD will then drop this request (As it exceeds the 10mb limit) and will not show the payloads.

Changing how many payloads the DataPower will batch together

Both the number of transactions DataPower groups and sends to DPOD with each batch and the maximum batch size are configurable **in DPOD** (and not in the DataPower).

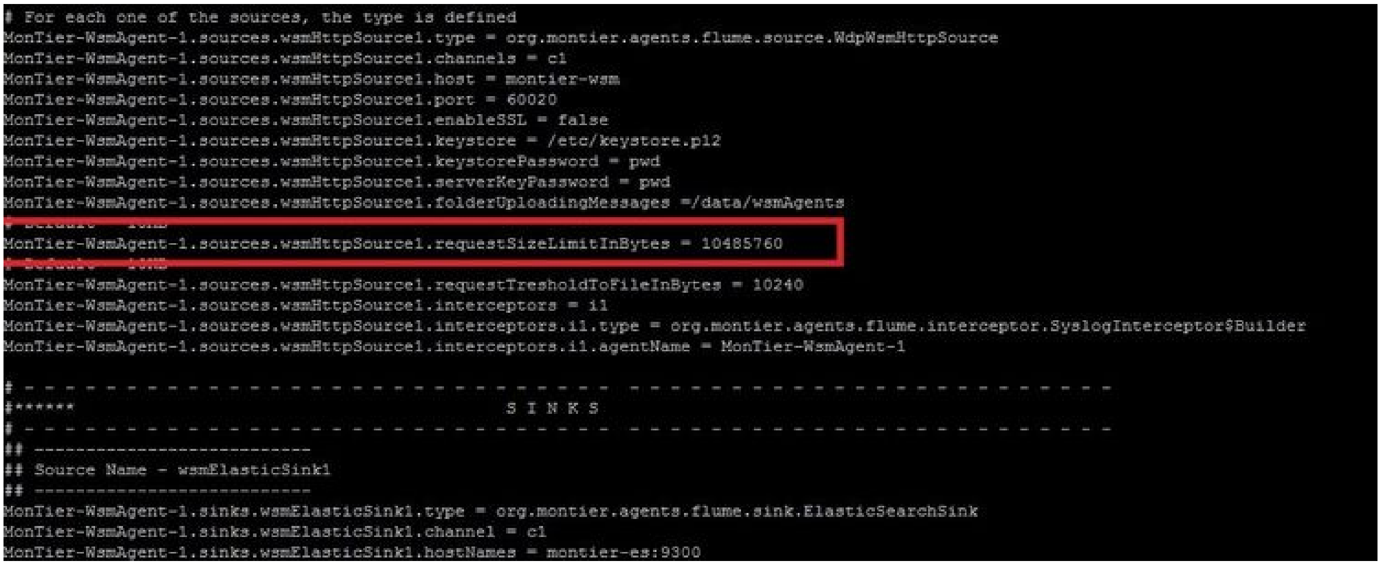
Change the following system parameters:
WS-M Subscription Push Max Elements - Number of transactions DataPower groups together (the default is 20)
WS-M Subscription Max Envelope Size - Maximum batch size that the DataPower will send to DPOD (the default is 10485760 = 10mb)

Changing the max batch size DPOD can handle

> You will need to stop DPOD WSM agent from the CLI before changing the following values, and restart it afterwards.

edit **/app/flume/wsm_agents/conf/MonTier-WsmAgent-X/flume_wsm.conf** (where **X** is the number of the WSM Agent you want to effect)

The relevant configuration key is:
MonTier-WsmAgent-**X**.sources.wsmHttpSource1.requestSizeLimitInBytes - max batch size that DPOD will process (the default is 10485760 = 10mb)

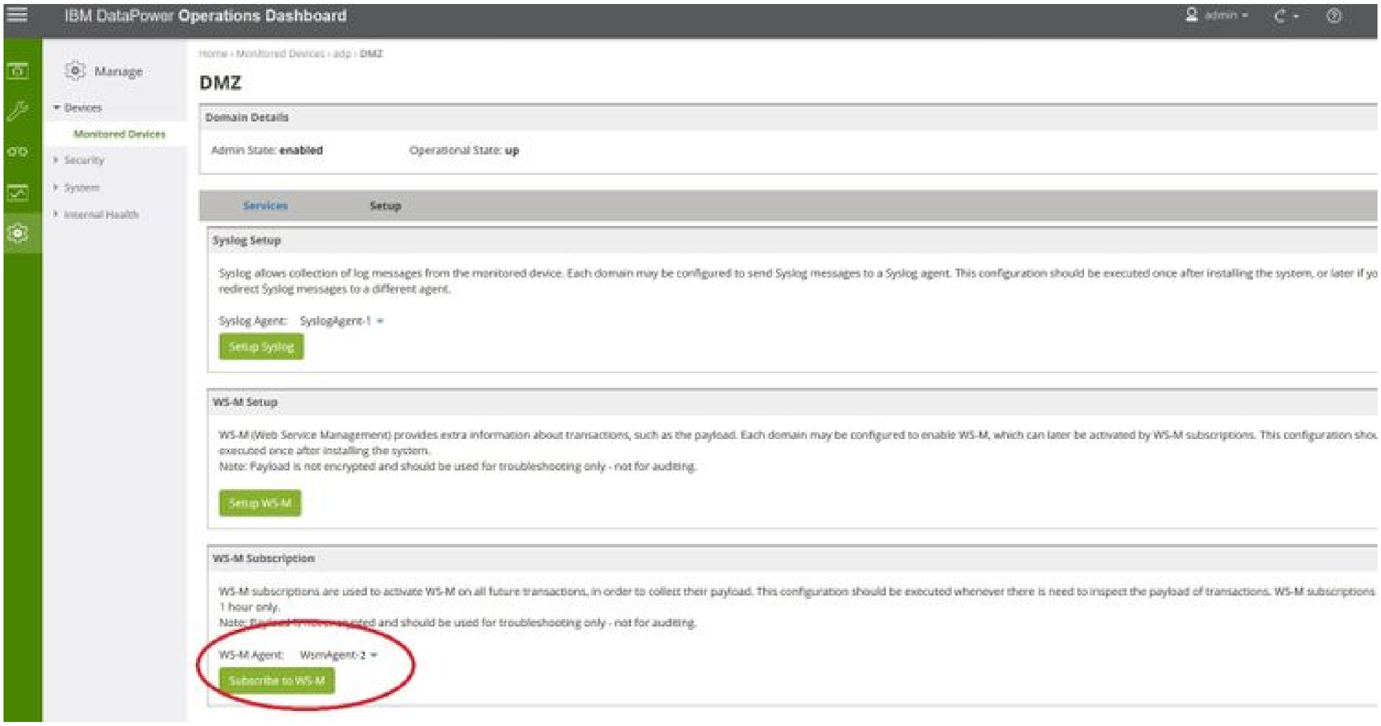


```
# For each one of the sources, the type is defined
MonTier-WsmAgent-1.sources.wsmHttpSource1.type = org.montier.agents.flume.source.WdpWsmHttpSource
MonTier-WsmAgent-1.sources.wsmHttpSource1.channels = c1
MonTier-WsmAgent-1.sources.wsmHttpSource1.host = montier-wsm
MonTier-WsmAgent-1.sources.wsmHttpSource1.port = 60020
MonTier-WsmAgent-1.sources.wsmHttpSource1.enableSSL = false
MonTier-WsmAgent-1.sources.wsmHttpSource1.keystore = /etc/keystore.p12
MonTier-WsmAgent-1.sources.wsmHttpSource1.keystorePassword = pwd
MonTier-WsmAgent-1.sources.wsmHttpSource1.serverKeyPassword = pwd
MonTier-WsmAgent-1.sources.wsmHttpSource1.folderUploadingMessages =/data/wsmAgents
# Default - 10MB
MonTier-WsmAgent-1.sources.wsmHttpSource1.requestSizeLimitInBytes = 10485760
# Default - 10KB
MonTier-WsmAgent-1.sources.wsmHttpSource1.requestTresholdToFileInBytes = 10240
MonTier-WsmAgent-1.sources.wsmHttpSource1.interceptors = i1
MonTier-WsmAgent-1.sources.wsmHttpSource1.interceptors.i1.type = org.montier.agents.flume.interceptor.SyslogInterceptor$Builder
MonTier-WsmAgent-1.sources.wsmHttpSource1.interceptors.i1.agentName = MonTier-WsmAgent-1

# - - - - - - - - - - - - - - - - - - - - - - - - - - - -  - - - - - - - - - - - - - - - - - - - - - - - -
#******                                        S I N K S
# - - - - - - - - - - - - - - - - - - - - - - - - - - - -  - - - - - - - - - - - - - - - - - - - - - - - -
## ----------------------------
## Source Name - wsmElasticSink1
## ----------------------------
MonTier-WsmAgent-1.sinks.wsmElasticSink1.type = org.montier.agents.flume.sink.ElasticSearchSink
MonTier-WsmAgent-1.sinks.wsmElasticSink1.channel = c1
MonTier-WsmAgent-1.sinks.wsmElasticSink1.hostNames = montier-es:9300
```

Best Practices

It is better to lower the number of the batched payloads (wdp.wsm.push.max_elements) than to increase the batch size DPOD can accept (wdp.wsm.push.max_envelope_size and wsmHttpSource1.requestSizeLimitInBytes). Making more smaller requests allows both the DataPower and DPOD to work in parallel and requires less memory on both appliances. Specifically, setting wsmHttpSource1.requestSizeLimitInBytes to a high value may put some stress on DataPower and DPOD machines with a low amount of RAM.

In cases where specific transaction/batch of transaction is larger than 10mb, try and raise the limit only for one specific WS-M agent and selecting this agent when subscribing to WS-M.



DMZ

Domain Details

Admin State: **enabled** Operational State: **up**

Syslog Setup

Syslog allows collection of log messages from the monitored device. Each domain may be configured to send Syslog messages to a Syslog agent. This configuration should be executed once after installing the system, or later if yo
redirect Syslog messages to a different agent.

Syslog Agent: SyslogAgent-1

WS-M Setup

WS-M (Web Service Management) provides extra information about transactions, such as the payload. Each domain may be configured to enable WS-M, which can later be activated by WS-M subscriptions. This configuration shou
executed once after installing the system.
Note: Payload is not encrypted and should be used for troubleshooting only - not for auditing.

WS-M Subscription

WS-M subscriptions are used to activate WS-M on all future transactions, in order to collect their payload. This configuration should be executed whenever there is need to inspect the payload of transactions. WS-M subscriptions
1 hour only.
Note: Payload is not encrypted and should be used for troubleshooting only - not for auditing.

WS-M Agent: WsmAgent-2

Policy Variables Capture Settings and Authorization

AUTHORIZATION TO CREATE NEW CAPTURES

DPOD lets users create new Policy Variables Capture from the Policy Variables Capture Page
This page will be accessible to the following users:

- Admins (users with the OpDashAdminRole Role)
- Users that has a custom role with "Allow Manage API-C Policy Variables Captures" set to Yes

AUTHORIZATION TO VIEW POLICY VARIABLES TRACE

The variables names and values are viewable in the Policy Details Window (when drilling down to a single API-C transaction)
The data will be accessible to the following users:

- Admins (users with the OpDashAdminRole Role)
- Users that has a custom role with "Allow Viewing API-C Policy Variables" set to Yes

AUTOMATIC DELETION FROM STORE

Policy Variables data can be automatically deleted from store after one day or one week - see "Time to Keep WS-M Payloads" in system parameters (the same parameter controls both WS-M payloads and Policy Variables).
If this value is not set, data will be deleted when the store fills up (earliest ones will be deleted first), the exact time depends on your store allocation size

Considerations for GDPR readiness

IBM DataPower Operations Dashboard considerations for GDPR readiness

FOR PID(S): IBM DATAPOWER OPERATIONS DASHBOARD

- 5725-T06 IBM DataPower Gateway

NOTICE:

This document is intended to help you in your preparations for GDPR readiness. It provides information about features of IBM DataPower Operations Dashboard that you can configure, and aspects of the product’s use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

TABLE OF CONTENTS

Note: The links to the DataPower Gateway Knowledge Center in this document are for version 7.6. If you are using a different version, use the "Change version" option in IBM Knowledge Center to change to the appropriate version of the topic.

GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union (“EU”) and applies from May 25, 2018.

Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing of personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

Read more about GDPR

EU GDPR Information Portal

ibm.com/GDPR website

PRODUCT CONFIGURATION FOR GDPR

How to configure our offering such that it could be used in a GDPR environment?

User configuration

After deployment and installation of DataPower Operations Dashboard you will need to become familiar with its role-based access control. By default, DataPower Operations Dashboard uses internal users and group registries to facilitate the user administration for nonproduction scenarios.

Restrict the creation of internal users by using a Lightweight Directory Access Protocol (LDAP) user registry. In the external registry, assign users to groups and assign groups to roles. When appropriately defined, the access policy controls which users in which roles can access which resources.

Starting with DataPower Operations Dashboard v1.0.8, the management of local users is disabled as it is not supported in production environments because it is a less secured practice.

Restrict the `admin` group to the specific IP addresses in product configuration and firewalls and protect its credentials.

Review the product recommendations for post installation task that are recommended in hardening installation and to improve the product security such as replacing self-signed certificates, implement SSL Client Authentication with the gateway, and so forth. In each version, this list is updated. Review this documentation after an upgrade.

Management services configuration

After the installation of DataPower Operations Dashboard is complete, you will need to modify and enable the following:

1. Replace self-signed certificates as they are used for the web console and the REST management service.
2. Implement SSL Client Authentication with the Gateway Management services (SOAP/REST) to secure data.
3. If you suspect that that the syslog payload data contains private information, encrypt your drives and file systems.
4. If you plan to expose DataPower Operations Dashboard web console to API developers that are located on other network segments than your gateways, use the External Web console to avoid granting access through firewalls to the DataPower Gateway network segments.
5. You should consider separating your DataPower Operations Dashboard installation into production and nonproduction environments and bind only the production gateways to the production DataPower Operations Dashboard installation to minimize access to personal data.
6. You should consider using masked data in nonproduction environments in case you execute transactions based on data originated from production environments.

Transaction services configuration

After the installation of the DataPower Operations Dashboard is complete, you will need to configure each gateway (known as *monitored device*) from the DataPower Operations Dashboard web console. The configuration requires that you provide a privileged user to access and configure the gateway.

Create a dedicated user and grant only the privileges that you want DataPower Operations Dashboard to perform.

After a gateway is added to the DataPower Operations Dashboard management list, all transaction information starts to be pushed to DataPower Operations Dashboard. By default, DataPower Operations Dashboard does not configure the syslog log targets on the DataPower Gateway to push data over a secured connection. You must configure these required steps manually.

Payload capture is disabled by default. Do not enable this feature in the DataPower Gateway, and do not configure the WS-Management Agent on a monitored device level in the DataPower Gateway. If a DataPower Operations Dashboard administrator configures the capture of payloads, this data is pushed to DataPower Operations Dashboard over an unsecured transport, and it is not encrypted at rest in DataPower Operations Dashboard.

If you still want to capture payload data for limited time for debug purposes ensure the following setup:

1. Your disks and file system are encrypted.
2. Enable specific domain in your DataPower Gateway to be able to capture payload.
3. Create a capture subscription for a limited time (for example 5-10 minutes) and for a specific DataPower Gateway domain.
4. Review and adjust DataPower Operations Dashboard user's custom role to grant only those required to see payloads.
5. Keep payload for the shortest time possible in order to minimize risks.
6. Enable auto-delete of payloads and and set a threshold of a few minutes.
7. Delete all payload data after you finish your troubleshooting.

If you offload any data from DataPower Operations Dashboard, encrypt them as they might contains personal data.

DATA LIFE CYCLE

What is the end-to-end process through which personal data go through when using our offering?

User Accounts

DataPower Operations Dashboard provides access to the management of Users, Groups and Role-Based managed security mechanism via its Manage and Security options. This can be done when managing users using DataPower Operations Dashboard internal database registry. It is not available when LDAP is the selected option for managing those users.

Avoid using the local user registry , and use instead LDAP repositories to manage your users.

System Logs

Personal data, including IP addresses, session IDs, user IDs, webpage URLs, and cookie names, can exist in system logs. DataPower

Operations Dashboard collects and logs IP addresses, user and system names, and other *unstructured* data.

Messages in log files are captured automatically as part of the offering but can be controlled by the client. Log files are retained on disk. Log files cannot be modified but can be deleted. Log files are readily available for your review and monitoring.

Information about system logs and error reports is documented in the DataPower Gateway Knowledge Center. * For additional details about log files, see Log files.

- For additional details about error reports, see Error reports.

Data is collected from the DataPower Gateway as it is captured through the different interfaces (XML management, syslog log target, WS-Management Agent) and processed by DataPower Operations Dashboard. DataPower Operations Dashboard can divide the data in unstructured and structured data.

- Structured data is the IP addresses and potential user names that identified the transactions.
- Unstructured data is the payload associated with that logging information.

After the transactions are processed, they are stored in DataPower Operations Dashboard databases for analysis. This data is accessible depending on the DataPower Operations Dashboard user roles

The data will be stored in DataPower Operations Dashboard database until the database is full, while old entries are purged automatically.

DATA STORAGE

How can the client control the storage of personal data?

Storage of account data

You can backup DataPower Operations Dashboard software, static configuration, and user configuration data in the DataPower Operations Dashboard database by using internal scripts. When you provide the destination for the backup file, you need to make sure that it is located in a protected area. For more information please refer to the documentation here.

DATA ACCESS

How can the client control access to personal data?

Security Roles

Security roles are used to provide a way for the administrator to filter the view that users have of the system. Administrators can use the roles to filter out data from user's view by devices, domains, services, client IP addresses, payload, and more. Filtering provides users with insights to only the parts of the system that they are allowed to access.

There are two types of security roles available with DataPower Operations Dashboard.

- Built-in roles that DataPower Operations Dashboard itself uses. These roles cannot be added, deleted, or modified.
- Custom roles that are defined by the DataPower Operations Dashboard administrator. These roles can be added, deleted, or modified by a DataPower Operations Dashboard administrator.

Data can be accessed in two main ways.

- The web console that is controlled by DataPower Operations Dashboard access control.
- Directly by the system administrator to files that should be controlled by the client by using proper policies of credential keeping, firewall access, and physical access to the offering servers. The administrator has the following access: *readaccess*, *writeaccess*, *update_access* .

Separation of duties

Separation of duties can be applied by using the security roles that are both built-in and custom.

Privileged Administrators

Administrator access can be filtered by IPs, but client should enforce network access management such as firewalls and network segment separation. Customers should pay attention to the ability to access the CLI level using SSH.

Activity logs

Access logs to the web console are generated by the offering. However, system admins with CLI access can delete these files.

DATA PROCESSING

How can the client control processing of personal data?

DataPower Operations Dashboard cannot anticipate which data is personal data and which data is generated from the processing of the transactions. If transactions contain personal data, the client must properly identify this type of data and to protect this data if transferred off of DataPower Operations Dashboard.

DATA DELETION

How can the client control the deletion of personal data?

DataPower Operations Dashboard cannot anticipate which data is personal data and which data is generated from the processing of the transactions. If transactions contain personal data, the client must properly identify this type of data in order to delete it. Once the data has been identified, client should perform the following steps to ensure complete removal of the data from the DataPower Operations Dashboard:

1. Locate and replace or delete system log files that contain information that is identified as personal data.
2. Locate transactions that contain personal data using Raw Messages dashboard and delete all transactions with personal data.
3. Delete all exported data such as Backups, Reports, and all other offloaded data that might contain personal data.
4. Delete entire data according to its type (Syslogs, payloads etc.)

DATA MONITORING

How could the client monitor the processing of personal data?

- DataPower Operations Dashboard does not monitor log files.

DataPower Operations Dashboard provides many dashboards to explore and search the information that is being captured. However, this offering primarily gathers unclassified data, for there is no way to anticipate whether the log data contains personal data.

DataPower Operations Dashboard cannot monitor the processing of personal data in specific beyond the overall health monitoring of the offering. DataPower Operations Dashboard contains internal health monitoring and alerts to monitor its component health. However, this monitoring does not monitor the DataPower Operations Dashboard system logs.

CAPABILITY FOR RESTRICTING USE OF PERSONAL DATA

Will your customers be able to address Data Subject requests from their customers?

DataPower Operations Dashboard meets the following data subject rights: right to access, modify, forgotten, and portability.

- For additional information about managing local user accounts, user groups, and access rights, see here.

The customer is responsible for meeting data subject rights through their database application logic and business processes.

Reference

The information in the following sections describes.

- System Parameters List
- Report publishing Web-Service
- OS Kernel settings
- Setting Up a Development VM for DPOD Installation on VMWare
- APIs Documentation
- Appliance Maintenance Status Codes
- DevOps Services Portal's User Scripts

System Parameters List

IBM DataPower Operations Dashboard contains an extensive set of parameters that let administrators fine-tune the system's behavior to the installation requirements.
The following sections describe these parameters in detail.

The parameters are accessible through the System Parameters page: **[Manage->SystemSystem Parameters].**

Appliance Maintenance

The Appliance Maintenance (Backup, Sync and Firmware upgrade) system parameters are listed on a separate page

APM

Parameter	Category	Default Value	Description
APM Integration Syslog App Name	APM Integration	DPOD-MSC1	Logical name used by APM to indentify DPOD.
APM Integration Target Syslog Host	APM Integration	172.77.77.7	APM's IP address or hostname
APM Integration Target Syslog Port	APM Integration	60030	APM's listening port
APM Integration Target Syslog Protocol	APM Integration	tcp	APM's listening protocol for Syslog
APM Integration Target Syslog SSL	APM Integration	false	Is conncetion secured?
APM Integration Events Publishing Enable	APM Integration	true	Activate / Disable integration between DPOD and APM installation.

Alerts

Parameter	Category	Default Value	Description
Enable Queries Emails SMTP	Alerts	true	Enable / Disable publishing alerts via SMTP server
Enable Queries Emails SMTP WS	Alerts	false	Enable / Disable publishing alerts via Web Service
Fields to Ignore in ElasticSearch Response in Alerts	Alerts	doc_count_error_upper_bound,sum_other_doc_count	Field to omit from alert description
Enable Queries Output File	Alerts	false	Enable / Disable publishing alerts as file in local file system
Syslog Severity Field Value	Alerts	info	Syslog record message level. Possible values: debug, info, notice, warning, err, crit, alert, emerg
Alerts Syslog Server Hostname	Alerts	172.77.77.7	Syslog server hostname or IP address.
Alerts Syslog Server Port	Alerts	60031	Syslog server listening port.

Dashboards

Parameter	Category	Default Value	Description
IDG Transactions Page Columns	Dashboards	Service Name, Operation, Time, Device, Domain, Status, Transaction ID, Client IP, Global Transaction ID, Elapsed, Payload	Controls which columns will appear in the Investigate->Transactions Page, you can omit or reorder the columns. Any mistakes in the input will cause the display to revert to the default value. The Payload field will not appear to users that does not have authorization to view payloads Possible values (not case sensitive): Service Name, Operation, Time, Device, Domain, Status, Transaction ID, Client IP, Global Transaction ID, Elapsed, Payload

IDG Raw Message Page Columns	Dashboards	Device, Domain, Category, Severity, Time, Direction, Object Type, Object Name, Transaction ID, Client IP, Message Code, Message	Controls which columns will appear in the InvestigateRaw Messages Page, you can omit or reorder the columns. Any mistake in the input will cause the display to revert to the default value. Possible values (not case sensitive): Device, Domain, Category, Severity, Time, Direction, Object Type, Object Name, Transaction ID, Client IP, Message Code, Message, Global Transaction ID, B2B Message ID, B2B From Partner ID, B2B to Partner ID, B2B from partner profile, B2B to Partner Profile,
APIC Transactions Page Columns	Dashboards	API Name, Time, Device, Catalog Name, Space Name, Operation ID, Client ID, OAuth Scope, Status, Transaction ID, Client IP, Global Transaction ID, Elapsed, Payload	Controls which columns will appear in the APIC Investigate->Transactions Page, you can omit or reorder the columns. Any mistakes in the input will cause the display to revert to the default value. The Payload field will not appear to users that does not have authorization to view payloads Possible values (not case sensitive): API Name, Time, Device, Catalog Name, Space Name, Operation ID, Client ID, OAuth Scope, Status, Transaction ID, Client IP, Global Transaction ID, Elapsed, Plan Name, Domain, Payload
Service URI Dashboard Percentiles (3 comma separated decimals)	Dashboards	90.0, 95.0, 99.0	Controls the percentiles shown in the rightmost columns of the Service URI Calls page and the API URI calls page, enter decimal values between 0-99.9
Service URL Dashboard Percentiles (3 comma separated decimals)	Dashboards	90.0, 95.0, 99.0	Controls the percentiles shown in the rightmost columns of the Service URL Calls page and the API URL calls page, enter decimal values between 0-99.9
APIC Recent Activity Page Latency Percentile	Dashboards	90.0	Controls the percentile shown in the APIC Recent Activity page, enter a decimal value between 0-99.9

Device Health

Parameter	Category	Default Value	Description
System Health Dashboard Sample Time Range (min.)	Device Health	5	See "Device Health Calculation" in System Health

Reports

The following parameters determine DPOD's reporting behavior.

Parameter	Category	Default Value	Description
Enable Reports Emails SMTP	Reports	true	Enables sending reports via SMTP
Enable Reports Emails SMTP WS	Reports	false	Enables sending reports via a Web-Service
Enable Reports Output File	Reports	false	Enables writing reports to a local file-system. (Defaults to /data/reports)
Fields to ignore in ElasticSearch response	Reports	doc_count_error_upper_bound,sum_other_doc_count	**For internal use, do not change unless instructed to do so by product support.**

For more information see reports or configuring sending reports in mail.

Emails and SMTP (For report publishing, alerts, share, maintenanace plans etc)

When sending notifications via SMTP or SMTP WS. the following parameters determine how those notifications are sent.

When SMTP or SMTP-WS is selected as the reporting behavior, all parameters relating this behavior must be provided.

Parameter	Category	Default Value	Description
From Address	Email	from@example.com	The from address used for the report email.
SMTP Host	Email SMTP	smtp.example.com	Destination SMTP host

SMTP Password	Email SMTP	********	Password for logging in to the SMTP host. If no authentication required leave this field empty.
SMTP Port	Email SMTP	465	Destination SMTP host port
SMTP User	Email SMTP	mailer@example.com	Username for logging in to the SMTP host. If no authentication required leave this field empty.
SMTP SSL Enabled	Email SMTP	true	Enable / Disable TLS/SSL
SMTP WS Endpoint URI	Email SMTP WS	/SMTPSender	Destination URI for sending reports via Web-Service
SMTP WS Host	Email SMTP WS	localhost	Destination hostname for sending reports via Web-Service
SMTP WS Port	Email SMTP WS	8080	Destination port for sending reports via Web-Service
SMTP WS Protocol	Email SMTP WS	HTTP	Protocol for accessing the Web-Service host Valid values: HTTP / HTTPS
SMTP WS User	Email SMTP WS	user	User used for sending reports via Web-Service. This value is sent using HTTP Basic Authentication.
SMTP WS Password	Email SMTP WS	********	Password used for sending reports via Web-Service. This value is sent using HTTP Basic Authentication.

See reports for more information

LDAP

The following parameters control configuration and connection to LDAP, used for role-based security.

All parameters below are mandatory when enabling LDAP role-based security (by switching on the **Enable LDAP** parameter).
If LDAP RBM is disabled, all these parameters should be left blank.

Parameter	Category	Default Value	Description
LDAP Connection Name (DN)	LDAP		Username for connecting to the LDAP server (sometimes called “bind user”)
LDAP Connection PASSWORD	LDAP		Password for connecting to the LDAP server
LDAP Connection URL (ldap://IP:Port)	LDAP		Connection URL to connect to the LDAP server
Enable LDAP	LDAP	false	Whether the LDAP RBM is enabled. Valid Values: true / false
LDAP Group Base Entry (e.g. OU)	LDAP		The top-most level of the LDAP hierarchy. Searching for LDAP groups starts from this point downward. Ensure the user configured above is authorized to connect to this point in the LDAP hierarchy.
LDAP Group Name Attribute	LDAP		LDAP Group Name Attribute
LDAP Group Search Filter ({0} - Authenticated User Name, {1} - Authenticated User DN)	LDAP		The LDAP filter expression to use when searching for a group's directory entry
LDAP Referral (ignore/follow)	LDAP	ignore	Define handling of JNDI referrals (see javax.naming.Context.REFERRAL for more information). Valid values are: • ignore • follow • throw Microsoft Active Directory often returns referrals. Set this parameter to **follow** If your installation is required to follow them. Caution: if your DNS is not part of AD, the LDAP client lib might try to resolve your domain name in DNS to find another LDAP server.

LDAP User Base Entry (e.g. OU)	LDAP		The top-most level of the LDAP hierarchy. Searching for LDAP users starts from this point downward. Ensure the user configured above is authorized to connect to this point in the LDAP hierarchy.
LDAP User Search Filter ({0} - User Name)	LDAP		The LDAP filter expression to use when searching for a user's directory entry

For more information regarding DPOD and LDAP configuration, consult the sections under Configuring LDAP in the Admin Guide.

Monitored Devices Authentication

The following parameters control authentication of monitored DataPower Gateways.
When DPOD collects data from monitored devices, it verifies that these are the correct devices using TLS; The DataPower certificate is authenticated against DPOD's CA trust store, specified below.

Parameter	Category	Default Value	Description
Local User Registry Enabled	Security	false (for new installations v1.0.7+) true (when upgrading from v1.0.6)	When disabled, DPOD will not store any **new** user details in local repository to comply with Security complaince requirements (DPOD will not automatically delete any existing user details after changing the value of this parameter)
TLS Level (TLSv1/TLSv1.1/TLSv1.2)	Security	TLSv1.2	TLS level used to perform authentication
CA Trusted Keystore Password	Security		Trust store password
CA Trusted Keystore Full Path and Filename	Security	/app/java/jre/lib/security/cacerts	Trust store full path
CA Trusted Keystore Type (JKS/PKCS12)	Security	JKS	Trust store type

TLS configuration information can be found in LDAP Configuration Script.

Configuration changes tracking

DPOD collects data about DataPower configuration changes from its monitored devices. It does this by pulling the complete configuration from the device, and comparing it to the last collected configuration. The parameters below control this mechanism.

Parameter	Category	Default Value	Description
Interval time to extract all service configuration and compare to last version; In Seconds;	ServiceConfig	1800	Determines how often monitored devices configuration is collected and compared to the last version. Recommended nterval is at least 900 (15 minutes).
Interval number to compress Configuration Table since massive update and delete occurs. Once a day	ServiceConfig	50	**For internal use, do not change unless instructed to do so by product support.**

Consult the table on System Services Management for more information about the types of agents in DPOD and the information they collect.

Console UI Appearance

These parameters control the way data is displayed in DPOD's Console UI.

Parameter	Category	Default	Description
Default Full Date Format	Style	MM/dd/yyyy HH:mm:ss.SSS	Full date format
Default Date Format with no Millis	Style	MM/dd/yyyy HH:mm:ss	Full date format, without milliseconds
Default Date Format with no Year	Style	MM/dd HH:mm:ss.SSS	Full date format, without year
Default Short Date Format	Style	MM/dd/yyyy	Short date format

Default Theme (light/dark/elegant)	Style	Light	Light, dark or elegant theme of the console UI screens

Internal Health

> Changes to the following parameters will take affect only after restarting the keepalive service via app-util.sh

Parameter	Category	Default	Description
Internal Alerts - Check Agents Interval in Seconds	Health	300	How often to check whether DPOD's syslog and WS-M agents are up and working
Internal Alerts - Check Derby Interval in Seconds	Health	300	How often to check whether DPOD's internal database is up and working
Internal Alerts - Check Dropped Syslogs Interval in Seconds	Health	600	How often to check whether DPOD's syslog agents lost incoming messages
Internal Alerts - Check Dropped WS-M Messages Interval in Seconds	Health	600	How often to check whether DPOD's WS-M agents lost incoming payloads
Internal Alerts - Check ES Interval in Seconds	Health	300	How often to check whether DPOD's big data component is up and working
Internal Alerts - Check File System Interval in Seconds	Health	300	How often to check whether DPOD's filesystem is out of space
Internal Alerts - Check Retention Interval in Seconds	Health	300	How often to check whether DPOD's internal big data retention process is working
Internal Alerts - Send Email on Alert	Health	false	Whether or not to send an Email when a problem was detected by the internal health monitoring
Internal Alerts - Email Destination Address for Alerts	Health	No Default	Destination Email address for sending internal health alerts
Internal Alerts - Send Syslog on Alert	Health	false	Whether or not to send a Syslog message when a problem was detected by the internal health monitoring
Interval in Seconds to Sample Logging Targets	Health	300	How often to sample DPOD's log targets in the monitored devices
Interval in Seconds to Sample Nodes Health Statistics	Health	300	How often to collect statistics on DPOD's big data nodes
Interval in Seconds to Monitor Objects Status	Health	300	How often to monitor enabled but down objects in the monitored devices
Object Status Monitor Should Only Check Common Object Classes	Health	true	By default, the Failed Objects dashboard (under the "explore" menu) displays only common object classes, set this option to false to make it sample all object classes in the monitored devices
Interval in Seconds to Sample WSM Agents Statistics	Health	300	How often to sample WS-M Agents in the monitored devices
Internal Alerts REST API Service Host	Health	localhost	Host name / IP address of the maintenance housekeeping server to save and publish internal alerts.
Internal Alerts REST API Service Port	Health	8084	Port of the maintenance housekeeping service to save and publish internal alerts.

DevOps Portal Parameters

Parameter	Category	Default	Description
Path and Name of Local WSDL Analyze Script	ServicesPortal	/app/custom/scripts/download_wsdl_artifacts_sample.py	The path and name of the user configurable python script for analyzing local WSDL
Path and Name of Local WSDL Replace Script	ServicesPortal	/app/custom/scripts/replace_wsdl_references_sample.py	The path and name of the user configurable python script for replacing local WSDL references
Enable Services Portal Operations for non-Admin Users	ServicesPortal	true	Enable or disable access of non-admin users to DevOps portal actions

Temporary Device Name for WSDL Validations Operations	ServicesPortal	(no default)	Device name that will be used to create temporary services for WSDL validations, the device must be monitored by DPOD
Temporary Domain Name for WSDL Validations Operations	ServicesPortal	(no default)	Temporary domain name that will be used to create temporary services for WSDL validations The domain needs to exist, DPOD will not create it
Local WSDL Files Max Upload Size in KB	ServicesPortal	300	Upload size limit for each WSDL or XSD file used in Local WSDL Validation/Promotion. Change will take effect after hitting refresh in the browser's window.
Import Service Max Upload File Size in KB	ServicesPortal	10000	Upload size limit for the import file in KB
Import Service Deployment Policies Path	ServicesPortal	/tmp	The dropdown with the selection of deployment policy files will be read from this folder (ZIP, XML and XCFG files only)
Service Import Temp Working Path	ServicesPortal	/app/tmp/servicesportal/import	Import files and deployment policies will be copied and processed in this folder
Path and Name of Import Service Validation Script	ServicesPortal	/app/custom/scripts/import_service_validation.py	The path and name of the user configurable python script for validating the import file
Path and Name of Import Service Deployment Policy Script	ServicesPortal	/app/custom/scripts/import_service_deppolicy_selector.py	The path and name of the user configurable python script for overriding the user selected deployment policy
Deployment Policy is Mandatory for Import Service	ServicesPortal	true	Is deployment policy mandatory for imports

Custom/Logical Transaction

Parameter	Category	Default	Description
Allow Monitoring Transactions in Default Domain	Transactions	false	Whether or not the "Support TX in the Default Domain" box will be displayed in the Monitored DevicesSetup page
Show Custom Transaction View Selection	Transactions	false	Whether or not the "Custom TX View" checkbox will be displayed in the Product Views
Default Transactions Source (syslog/logical)	Transactions	syslog	If the "Custom TX View" is displayed, what will be the default for users on their first sign in.
Logical Transaction, Custom String 1 Table Header	Transactions	Custom String 1	The Table Header and Filter names for "Custom String 1" in the transactions page
Logical Transaction, Custom String 2 Table Header	Transactions	Custom String 2	The Table Header and Filter names for "Custom String 2" in the transactions page
Transaction Analysis Level - User Override Path	Transactions	(blank)	Where to take the user override file for the syslog analysis message groups, no value (blank) means there is no override file
Transaction Analysis Level - Max TPS	Transactions	Core, MemoryReqRes, B2B, error	The message group names and log level for the Max TPS analysis level, The last parameter must be a valid log level name (debug, info, notice, warn. error, critic). The values must be comma separated, lower, upper or mixed case are allowed.
Transaction Analysis Level - More TPS	Transactions	Core, MemoryReqRes, B2B, notice	The message group names and log level for the More TPS analysis level, The last parameter must be a valid log level name (debug, info, notice, warn. error, critic). The values must be comma separated, lower, upper or mixed case are allowed.
Transaction Analysis Level - Balanced	Transactions	Core, MemoryReqRes, B2B, MemActionLevel, notice	The message group names and log level for the Balanced analysis level, The last parameter must be a valid log level name (debug, info, notice, warn. error, critic). The values must be comma separated, lower, upper or mixed case are allowed.
Transaction Analysis Level - More Data	Transactions	Core, MemoryReqRes, B2B, MemActionLevel, ReqPayloadSize, ExtLatency, info	The message group names and log level for the More Data analysis level, The last parameter must be a valid log level name (debug, info, notice, warn. error, critic). The values must be comma separated, lower, upper or mixed case are allowed.

Transaction Analysis Level - Max Data	Transactions	Core, MemoryReqRes, B2B, MemActionLevel, ReqPayloadSize, ExtLatency, Sidecalls, info	The message group names and log level for the Max Data analysis level, The last parameter must be a valid log level name (debug, info, notice, warn. error, critic). The values must be comma separated, lower, upper or mixed case are allowed.
Deprecated Extended Transaction Enabled	Transactions	false	If true system will show by defaut the Deprecated Extended Transaction page.

Miscellaneous Parameters

The following parameters control various other functions.

Parameter	Category	Default Value	Description
Enable agents management	Agents	true	Set to true, unless using an External Self Service Console installation, in which case it should be false.
Certificate monitoring duration in days	Certificate Monitoring	60	DataPower Gateways are able to send an alert a configurable number of days before certificates are about to expire. DPOD leverages this ability in the certificate monitoring screens. When a new monitored device is added to DPOD, the value in this parameter is copied to the corresponding parameter on the device. This value does not affect already-monitored devices. If you wish to change this in previously added devices, you need to do so manually.
Time to Keep WS-M Payloads (1d, 1w, blank)	WSM	(blank)	Automatically delete WS-M payloads from store, possible values are 1d = one day, 1w = one week, no value = don't delete automatically
Interval in Seconds to Sample Gateway MQ Objects Stats	WDP Objects	300	How often to sample the gateway's MQ objects, the data is shown in the Gateway MQ Overview dashboard

System Parameters

Parameter	Category	Default Value	Description
Is Internal Self Service Installation	System	true	Is the current DPOD installation an Internal Self Service Console - change this value only for external self service console scenarion
Internal Self Service Address	System	https://montier-management	The address of the internal Self Service Console - change this value only for external self service console scenarion
Internal Self Service User Name	System	(no default)	The DPOD user name that will be used to access the internal Self Service Console - change this value only for external self service console scenarion We recommend that you create a new user for this purpose
Internal Self Service Password	System	(no default)	The DPOD user's passwordthat will be used to access the internal Self Service Console - change this value only for external self service console scenarion
Internal Self Service Webserver Port	System	443	The internal Self Service Console's webserver port - change this value only for external self service console scenarion
Interval in Seconds to Check and Cleanup DB Tables	System	28800	Interval in seconds to cleanup DB tables that exceeded the threshold size (threshold for each table is defined in a different system parameter)
Threshold in MB to Clean Reports Execution Table	System	100	Threshold in MB to cleanup the reports execution DB table
Threshold in MB to Clean Alerts Execution Table	System	200	Threshold in MB to cleanup the alerts execution DB table
Threshold in MB to Clean Services Portal Execution Table	System	100	Threshold in MB to cleanup the services portal execution DB table
Threshold in MB to Clean Maintenance Plan Execution	System	100	Threshold in MB to cleanup the maintenance execution DB tables (backup, sync and firmware upgrade)
Experimental Features	Experimental	(no default)	For support use only, do not change unless advised by L2/L3 support

Report publishing Web-Service

DPOD may be configured to to send completed reports to a web-service. The web service itself is not provided by DPOD, and if you need to use this functionality, you will have to develop the receiving web service yourself.

This section describes the SOAP structure that DPOD emits, so that you may implement a service to receive it.

Some field values in the report web-service request are determined by system parameters. See the reporting and report publishing sections in System Parameters for more information.

Report Publishing Examples

Request Example

Request Example

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://MonTier/SMTPSender/">
    <soapenv:Header/>
    <soapenv:Body>
        <smt:SMTPRequest>
            <smt:ServerAddress>172.17.100.102</smt:ServerAddress>
            <smt:ServerPort>25</smt:ServerPort>
            <smt:To>kokomoko@gmail.com</smt:To>
            <smt:From>user1@montier.com</smt:From>
            <smt:Subject>mail test</smt:Subject>
            <smt:Body ><smt:/Body>
            <smt:Domain>montier.com</smt:Domain>
            <smt:FileName>Book1.xlsx</smt:FileName>

<smt:AttachmentType>application/vnd.ms-excel</smt:AttachmentType>

<smt:FileContent>UEsDBBQABgAIAAAAIQB8bJgWbAEAAKAFAAATAAgCW0NvbnRlbnRfVHl
wZXNdLnh...axwAAGRvY1Byb3BzL2NvcmUueG1sUEsFBgAAAAAMAAwADAMAAOEeAAAAAA==<
/smt:FileContent>
        </smt:SMTPRequest>
    </soapenv:Body>
</soapenv:Envelope>
```

Response Example

Response Example

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:smt="http://MonTier/SMTPSender/">
   <soapenv:Header />
   <soapenv:Body>
      <smt:SMTPRequest>
         <smt:Body />
         <smt:Domain>montier.com</smt:Domain>
         <smt:FileName>Book1.xlsx</smt:FileName>

<smt:AttachmentType>application/vnd.ms-excel</smt:AttachmentType>

<smt:FileContent>UEsDBBQABgAIAAAAIQB8bJgWbAEAAKAFAAATAAgCW0NvbnRlbnRfVHl
wZXNdLnh... ...
axwAAGRvY1Byb3BzL2NvcmUueG1sUEsFBgAAAAAMAAwADAMAAOEeAAAAAA==</smt:FileCo
ntent>
      </smt:SMTPRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Report Publishing Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://MonTier/SMTPSender/" version="1.00.00"
attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://MonTier/SMTPSender/">
   <xsd:element name="SMTPRequest">
      <xsd:complexType>
         <xsd:sequence>
            <xsd:element name="ServerAddress" type="xsd:string" />
            <xsd:element name="ServerPort" type="xsd:integer" />
            <xsd:element name="To" type="xsd:string" />
            <xsd:element name="From" type="xsd:string" />
            <xsd:element name="Subject" type="xsd:string" />
            <xsd:element name="Body" type="xsd:string" />
            <xsd:element name="Domain" type="xsd:string" />
            <xsd:element name="FileName" type="xsd:string" />
            <xsd:element name="AttachmentType" type="xsd:string" />
            <xsd:element name="FileContent" type="xsd:base64Binary" />
         </xsd:sequence>
      </xsd:complexType>
   </xsd:element>
   <xsd:element name="SMTPResponse">
      <xsd:complexType>
         <xsd:sequence>
            <xsd:element name="Result" type="xsd:string" />
         </xsd:sequence>
      </xsd:complexType>
   </xsd:element>
</xsd:schema>
```

Report Publishing WSDL

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
                  xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"

xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:tns="http://MonTier/SMTPSender/"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsdi="http://www.w3.org/2001/XMLSchema-instance"
                  targetNamespace="http://MonTier/SMTPSender/">
    <wsdl:types>
        <schema xmlns="http://www.w3.org/2001/XMLSchema">
            <import schemaLocation="SMTPSender.xsd"
namespace="http://MonTier/SMTPSender/" />
        </schema>
    </wsdl:types>
    <wsdl:message name="SMTPRequestMessage">
        <wsdl:part name="parameter" element="tns:SMTPRequest" />
    </wsdl:message>
    <wsdl:message name="SMTPResponseMessage">
        <wsdl:part name="parameter" element="tns:SMTPResponse" />
    </wsdl:message>
    <wsdl:portType name="SMTPSenderSoapPortType">
        <wsdl:operation name="SendSMTP">
            <wsdl:input message="tns:SMTPRequestMessage" />
            <wsdl:output message="tns:SMTPResponseMessage" />
        </wsdl:operation>
    </wsdl:portType>
    <wsdl:binding name="SMTPSenderSoapBinding"
type="tns:SMTPSenderSoapPortType">
        <soap:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document" />
        <wsdl:operation name="SendSMTP">
            <soap:operation soapAction="uri" />
            <wsdl:input>
                <soap:body use="literal" />
            </wsdl:input>
            <wsdl:output>
                <soap:body use="literal" />
            </wsdl:output>
        </wsdl:operation>
    </wsdl:binding>
    <wsdl:service name="SMTPSenderService">
        <wsdl:port name="SMTPSenderSoapPort"
binding="tns:SMTPSenderSoapBinding">
            <soap:address location="http://1.1.1.1/MonTier/SMTPSender"
```

```
/>
```

```
        </wsdl:port>
    </wsdl:service>
</wsdl:definitions>
```

OS Kernel settings

The DPOD Appliance installation configures various system and kernel settings in order to optimize performance and harden security.

Some of the settings has constant values and some are calculated during the Appliance installation based on the server (physical or virtual) resources, especially the amount of memory (RAM) the system has.

> It is highly important that on the Appliance OS installation phase the system will have all necessary resources allocated, especially the memory allocation.
>
> If You are installing Non-Appliance installation, a report listing system tests and gaps will be generated, please review the “kernel parameters” section and adjust you system to the recommended values, especially the performance related settings.
>
> This task is usually done by the Linux system administrator.

The following section details the most significant DPOD system settings:

Some of the parameters are based on the following calculations:

- system_page_size – usually 4096
- mem_bytes – system memory size in bytes
- shmmax=$mem_bytes * 0.90
- shmall=$mem_bytes / $system_page_size
- max_orphan=$mem_bytes * 0.10 / 65536
- file_max=$mem_bytes / 4194304 * 256
- max_tw=$file_max*2
- min_free=($mem_bytes / 1024) * 0.01

for SSD based hard drives

- vm_dirty_bg_ratio=5
- vm_dirty_ratio=15

for regular hard drives

- vm_dirty_bg_ratio=3
- vm_dirty_ratio=5

Performance related settings

- OS tuning

  # OS swaping behavior. vm.swappiness = 0 mean no swaping

  vm.swappiness = 0

  # kernel behavior with regard to the dirty pages

  vm.dirty_background_ratio = **$vm_dirty_bg_ratio**

  vm.dirty_ratio = **$vm_dirty_ratio**

- Network tuning

  # Basic TCP tuning

  net.ipv4.tcp_keepalive_time = 600

  net.ipv4.tcp_synack_retries = 3

  net.ipv4.tcp_syn_retries = 3

```
# Enable a fix for RFC1337 - time-wait assassination hazards in TCP
net.ipv4.tcp_rfc1337 = 1

# Minimum interval between garbage collection passes This interval is
# in effect under high memory pressure on the pool
net.ipv4.inet_peer_gc_mintime = 5

# Enable window scaling as defined in RFC1323
net.ipv4.tcp_window_scaling = 1
# Enable select acknowledgments
net.ipv4.tcp_sack = 1

# Enable FACK congestion avoidance and fast retransmission
net.ipv4.tcp_fack = 1

# Allows TCP to send "duplicate" SACKs
net.ipv4.tcp_dsack = 1

# Enable fast recycling TIME-WAIT sockets
net.ipv4.tcp_tw_recycle = 1

net.ipv4.tcp_max_syn_backlog = 20000

# tells the kernel how many TCP sockets that are not attached
# to any user file handle to maintain
net.ipv4.tcp_max_orphans = $max_orphan

# maximum number of sockets in TIME-WAIT to be held simultaneously
net.ipv4.tcp_max_tw_buckets = $max_tw

# don't cache ssthresh from previous connection
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1

# increase Linux autotuning TCP buffer limits
net.ipv4.tcp_rmem = 4096 87380 33554432
net.ipv4.tcp_wmem = 4096 65536 33554432

# increase TCP max buffer (bytes)
net.core.rmem_max = 67108864
net.core.wmem_max = 67108864
net.core.netdev_max_backlog = 30000
net.core.somaxconn = 65000
```

Resources related settings

```
# required free memory
vm.min_free_kbytes = $min_free

# system open file limit
fs.file-max = $file_max

# Maximum shared segment size in bytes
kernel.shmmax = $shmmax

 # Maximum number of shared memory segments in pages
kernel.shmall = $shmall
```

Security related settings

```
# Network security hardening
kernel.exec-shield = 1
kernel.randomize_va_space = 2
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.tcp_syncookies = 1
```

General settings

```
# Defines the local port range that is used by TCP and UDP
net.ipv4.ip_local_port_range = 1024 65535

# Enable timestamps (RFC1323)
net.ipv4.tcp_timestamps = 1
```

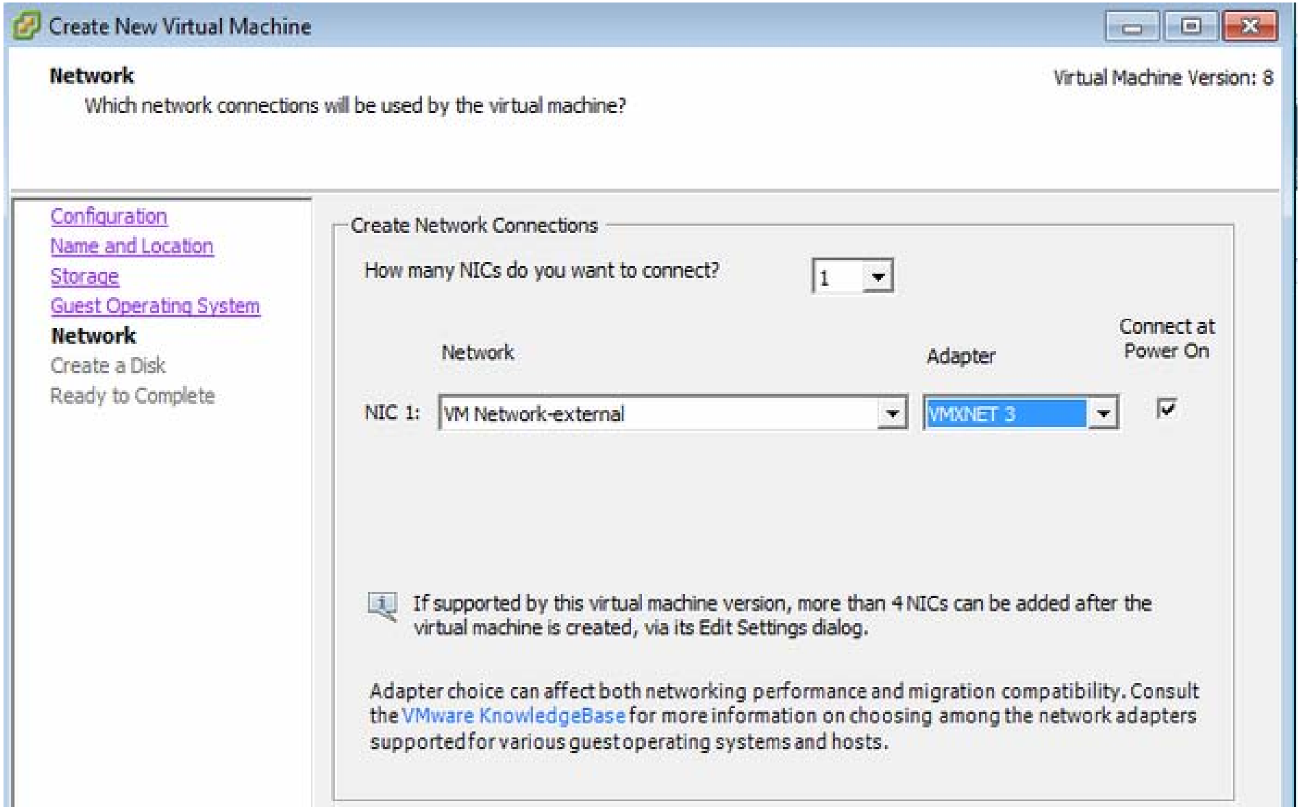
Limits configuration(/etc/security/limits.conf)

```
    *       hard    nofile      125000
    *       soft    nofile      125000
    root     hard    nofile      400000
    root     soft    nofile      400000
```

Setting Up a Development VM for DPOD Installation on VMWare

The information in this page provides a walk-through of the process you will need to follow in order to create a development VM for DPOD.

1. Using the vSphere client, create a new virtual machine, selecting the “Typical” configuration.
2. Provide a name for your new virtual machine (Any name will do)
3. Select the data store for the new virtual machine (the one planned for Disk 1). Consult Operating System (OS) to ensure it has enough free space.
4. Select the guest operating system “linux -> CentOS 4/5/6/7 (64bit)”.
5. Choose the number of network interfaces as described in the Network Requirements section. Ensure to check the "connect on power on" checkbox. (Note: DPOD is normally tested with Adapter type "VMXNET 3")



Create New Virtual Machine

Network
Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

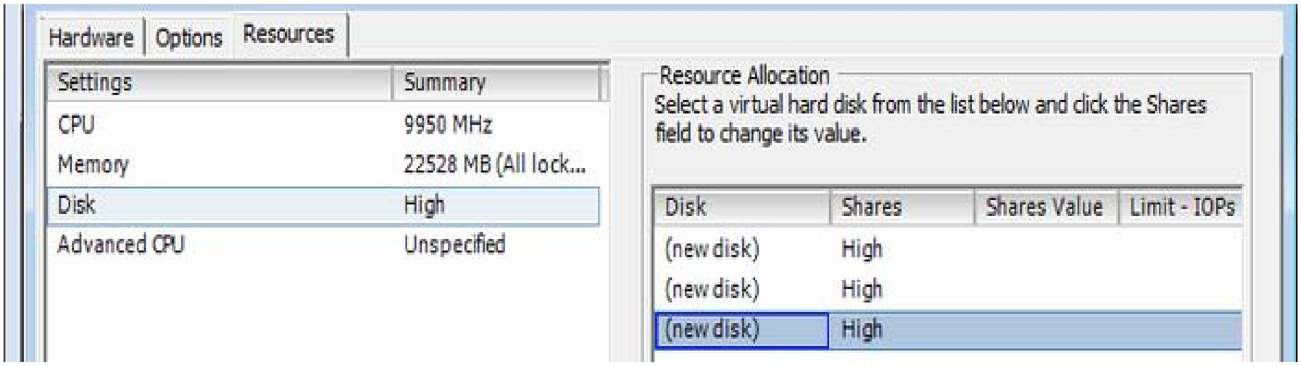
How many NICs do you want to connect? 1

	Network	Adapter	Connect at Power On
NIC 1:	VM Network-external	VMXNET 3	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

6. Configure the **OS disk** (It is recommended to select Thick Provision Eager Zeroed). Ensure to check the "edit the virtual machine settings before completion" checkbox at the bottom of the page and press "continue".
7. If no errors encountered, the Virtual Machine Properties Dialog should display. Perform the following steps:
    a. Remove the **floppy disk**
    b. Add a **new disk for product installation** (Disk 2) with enough space as described in the prerequisites section.
        i. Thick Provision Eager Zeroed recommended
        ii. In Disk Advanced Options – set this disk to Independent and Persistent.
    c. Add **new disk for data** with space as described in the prerequisites section.
        i. Thick Provision Eager Zeroed recommended
        ii. To achieve the best performance, ensure the disk is on a dedicated datastore. As this is your database storage, it should be as fast as possible.
        iii. In Disk Advanced Options – set this disk to Independent and Persistent.
8. Configure the **virtual machine memory** as described in the prerequisites section.
9. Configure the **virtual machine cores** as described in the prerequisites section.
10. **Reserve storage** by changing disks shares to "High":



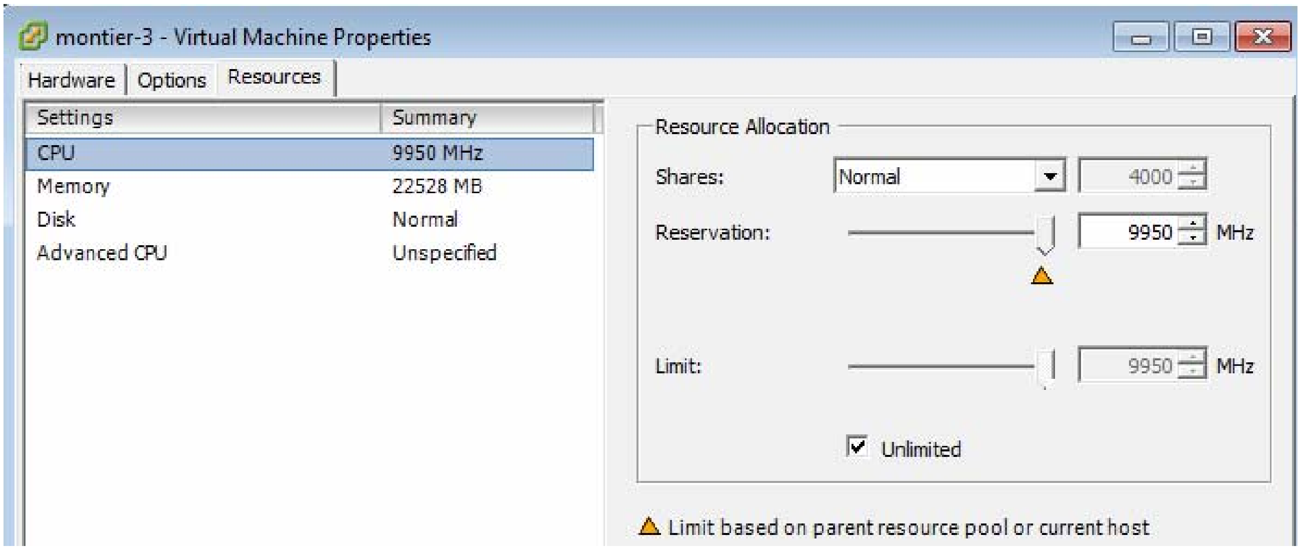
Settings	Summary
CPU	9950 MHz
Memory	22528 MB (All lock...
Disk	High
Advanced CPU	Unspecified

Resource Allocation

Select a virtual hard disk from the list below and click the Shares field to change its value.

Disk	Shares	Shares Value	Limit - IOPs
(new disk)	High		
(new disk)	High		
(new disk)	High		

11. **Reserve CPU** as much as possible:



Settings	Summary
CPU	9950 MHz
Memory	22528 MB
Disk	Normal
Advanced CPU	Unspecified

Resource Allocation

Shares: Normal 4000

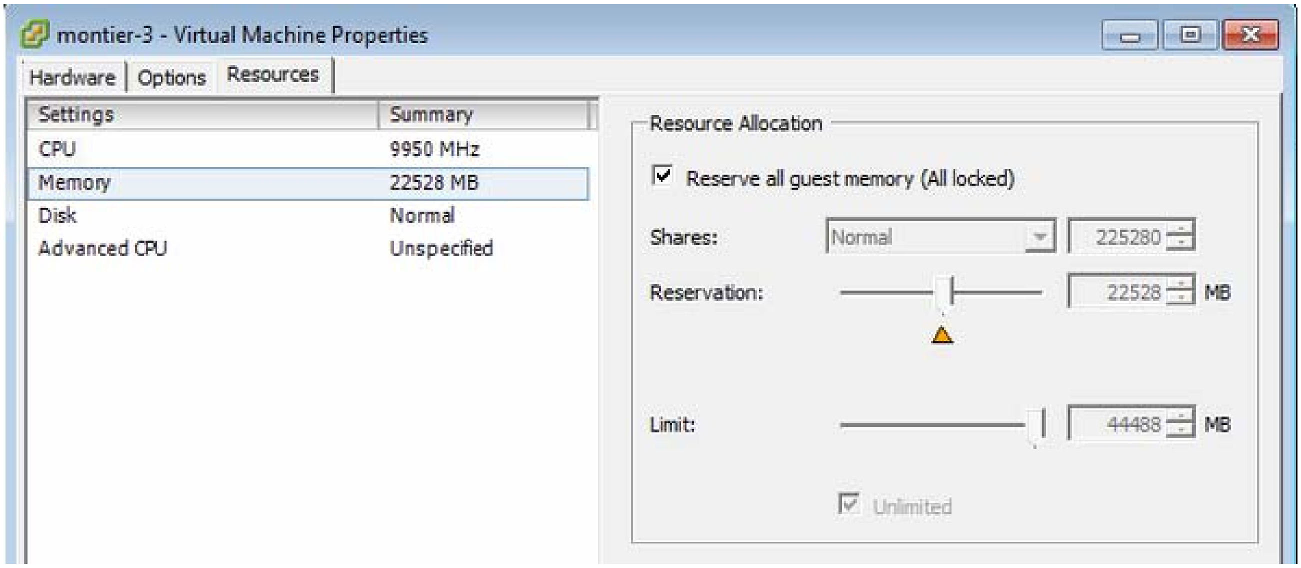
Reservation: 9950 MHz

Limit: 9950 MHz

☑ Unlimited

Limit based on parent resource pool or current host

12. **Reserve memory** as much as possible but no less than 20% from Guest allocation.



Settings	Summary
CPU	9950 MHz
Memory	22528 MB
Disk	Normal
Advanced CPU	Unspecified

Resource Allocation

☑ Reserve all guest memory (All locked)

Shares: Normal 225280

Reservation: 22528 MB

Limit: 44488 MB

☑ Unlimited

13. The DPOD installation is performed by booting an ISO image from CD/DVD. You will therefore need to configure the VM with CD/DVD:
    a. In The Virtual Machine Properties dialog choose new CD/DVD.
    b. You can use one of the 3 following options to connect to the ISO file:
        i. Upload the ISO to the ESXi. Select "Datastore ISO file" from the right panel and choose the datastore that has the DPOD All-In-One ISO file.
        ii. Use the host (ESXi) device so ask your ESXi administrator to put the DPOD All-In-One DVD in the DVD Drive.
        iii. Use your DVD in your Desktop where vSphere Client installed by choosing Client Device.
    c. Ensure to check the "connect at power on" checkbox.

APIs Documentation

- Alerts REST API
- Agents REST API
- Appliance Backup REST API
- Appliance Configuration Sync REST API
- Appliance Firmware Upgrade REST API
- Devices REST API
- DevOps Portal REST API
- DR REST API
- Reports REST API
- WS-M Subscription REST API
- Gateway/s REST API

Alerts REST API

User will need an opDashOperatorRole access for this API

Run alert by reference:

GET /op/api/v1/alerts/00000000-0000-0000-0000-a10000000001

```
{
"message": "Execution finished with no alerts.",
"esSearchResponse": {
"hits": {
"total": 0,
"hits": [],
"max_score": 0
},
"_shards": {
"total": 15,
"failed": 0,
"successful": 15
},
"timed_out": false,
"took": 236,
"aggregations": {
"terms1": {
"sum_other_doc_count": 0,
"buckets": [],
"doc_count_error_upper_bound": 0
}
}
},
"jsonQuery":
"{\"query\":{\"bool\":{\"must\":{\"match_all\":{}},\"filter\":{\"bool\":{\"must\":[{\"range\":{\"systemLoadTimeInMil\":{\"gte\":1486024160406,\"lte\":1486027760406}}}],\"must_not\":[]}}}},\"aggs\":{\"terms1\":{\"terms\":{\"field\":\"deviceName\",\"size\":1000,\"shardSize\":10000,\"order\":{\"max\":\"desc\"}},\"aggs\":{\"max\":{\"max\":{\"field\":\"usedCPUInPercentage\"}}}}},\"size\":0}",
"status": "OK",
"recipients": "someone@my-org.com",
"apiReference": "00000000-0000-0000-0000-a10000000001",
"queryName": "Devices_CPU",
"queryId": 1,
"filters": ":timeRangeType-recent:timeRangePeriod-3600000",
"threshold": 0
}
```

Example of an error:

```
{
"summary": "Exception:Reference test not found in QueryMetadata table
(org.montier.alerts.rest.QueryResource.executeQuery(QueryResource.java:58))",
"message": "Reference test not found in QueryMetadata table",
"status": "error"
}
```

Get all available alerts:

GET /op/api/v1/alerts/
The lastUpdateTime field returns the last time the alert was updated in epoch time format

```
{
"alerts": [
{
"name": "Devices_CPU",
"description": "Alert on Devices CPU over 80%",
"URI": "/op/api/v1/alerts/bc4353e3-7ba0-48e1-bc08-8b5cedf7d0cd",
"lastUpdateTime": 1513011809080
},
{
"name": "Devices_Memory",
"description": "Alert on Devices Memory over 70%",
"URI": "/op/api/v1/alerts/879b09f5-3bf4-47c6-88c0-51698294eab0",
"lastUpdateTime": 1487870145403
},
{
"name": "Devices_Load",
"description": "Alert on Devices Load over 80%",
"URI": "/op/api/v1/alerts/a43a6098-95bb-48fe-9b40-a226b2e22d3b",
"lastUpdateTime": 1487870145413
},
{
"name": "Devices_Fan",
"description": "Alert on Fan Health if less than 100%",
"URI": "/op/api/v1/alerts/b056372c-0222-431f-84ba-91b667bc4d13",
"lastUpdateTime": 1487870145420
},
{
"name": "Device_Temperature",
"description": "Alert on Temperature Health if less than 100%",
"URI": "/op/api/v1/alerts/935133bb-4b2f-4831-ad6f-d198995def76",
"lastUpdateTime": 1513581493084
}
]
}
```

Agents REST API

User will need an admin access for this API, Unauthorized users will get "401 Unauthorized"

Add Syslog agent:

```
POST /op/api/v1/agents/syslog?name=newAgent&host=someHost&port=1234&nodeName=N001&keepalive=true
{
  "resultCode": "OK"
}
```

error:

```
{
  "resultCode": "ERROR",
  "resultMessage": "Error - Name field is empty or null"
}
```

Add WS-M agent:

```
POST /op/api/v1/agents/wsm?name=newWsmAgent&host=someHost&port=1234&nodeName=N001&keepalive=true
{
  "resultCode": "OK"
}
```

error:

```
{
  "resultCode": "ERROR",
  "resultMessage": "Error - node not found"
}
```

Delete Syslog agent:

```
DELETE /op/api/v1/agent/syslog/someAgentName
{
  "resultCode": "OK"
}
```

error:

```
{
  "resultCode": "ERROR",
  "resultMessage": "Error - No Agents found with the name newAgent2"
}
```

Delete WS-M agent:

```
DELETE /op/api/v1/agent/wsm/someAgentName
{
  "resultCode": "OK"
}
```

error:

```
{
  "resultCode": "ERROR",
  "resultMessage": "Error - No Agents found with the name newWsmAgent1"
}
```

Appliance Backup REST API

Prerequisites

Requires admin or operator access.
Unauthorized requests will receive a "401 Unauthorized" response.

Send a backup plan to the execution queue:

POST /op/api/v1/backupplan/<API-Reference>/execute

The API-Reference of the plan is set in the add/edit plan page, and can be viewed in the plan details page

Successful Response

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Backup plan added to execution queue"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultErrorCode": "PLAN_NOT_FOUND",
"resultMessage": "Backup Plan with API Ref 199da450-7add-42fd-b644-986cfc018f32 was not found"
}
```

> This API call does NOT execute the plan, it just adds it to the execution queue.
> The plan may not be executed at all. (For example - when the current time is not within the plan's maintenance window timeframe, or if the plan is not enabled)

Get All Available Plans

GET /op/api/v1/backupplan/

The lastUpdateTime field returns the last time the plan was updated in epoch time format.

```
{
"plans": [
{
"name": "backup-QA",
"description": "Backup all QA Devices on Sundays",
"URI": "/op/api/v1/backupplan/199da450-7add-42fd-b644-986cfc018f31",
"lastUpdateTime": 1513582431660
},
{
"name": "backup-Prod",
"description": "Backup all PROD Devices daily",
"URI": "/op/api/v1/backupplan/199da450-7add-42fd-b644-986cfc018f31",
"lastUpdateTime": 1513582431660
}
]
}
```

Appliance Configuration Sync REST API

Prerequisites

Requires admin or operator access.
Unauthorized requests will receive a "401 Unauthorized" response.

Send a sync plan to the execution queue:

POST /op/api/v1/syncplan/<API-Reference>/execute

The API-Reference of the plan is set in the add/edit plan page, and can be viewed in the plan details page

Successful Response

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Sync plan added to execution queue"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultErrorCode": "PLAN_NOT_FOUND",
"resultMessage": "Sync Plan with API Ref 199da450-7add-42fd-b644-986cfc018f32 was not found"
}
```

> This API call does NOT execute the plan, it just adds it to the execution queue.
> The plan may not be executed at all. (For example - when the current time is not within the plan's maintenance window timeframe, or if the plan is not enabled)

Get All Available Plans

GET /op/api/v1/syncplan/

The lastUpdateTime field returns the last time the plan was updated in epoch time format.

```
{
"plans": [
{
"name": "SyncPlan1",
"description": "Sync from QA1 to QA2 and QA3",
"URI": "/op/api/v1/syncplan/6f56fa33-e201-47cb-aad5-be86d663e976",
"lastUpdateTime": 1513583061224
},
{
"name": "SyncPlan2",
"description": "",
"URI": "/op/api/v1/syncplan/d73d875c-adff-4cb3-90ab-7680b9662693",
"lastUpdateTime": 1505730217117
}
]
}
```

Appliance Firmware Upgrade REST API

Prerequisites

Requires admin or operator access.
Unauthorized requests will receive a "401 Unauthorized" response.

Send a firmware upgrade plan to the execution queue:

POST /op/api/v1/firmwareupgradeplan/<API-Reference>/execute

The API-Reference of the plan is set in the add/edit plan page, and can be viewed in the plan details page

Successful Response

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Firmware upgrade plan added to execution queue"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultErrorCode": "PLAN_NOT_FOUND",
"resultMessage": "Firmware upgrade plan with API Ref 199da450-7add-42fd-b644-986cfc018f32 was not found"
}
```

> This API call does NOT execute the plan, it just adds it to the execution queue.
> The plan may not be executed at all. (For example - when the current time is not within the plan's maintenance window timeframe, or if the plan is not enabled)

Get All Available Plans

GET /op/api/v1/firmwareupgradeplan/

The lastUpdateTime field returns the last time the plan was updated in epoch time format.

```
{
"plans": [
{
"name": "My Plan 1",
"description": "Just a test plan",
"URI": "/op/api/v1/firmwareupgradeplan/075D3780-4D79-4AFE-A749-817A3640C9E7",
"lastUpdateTime": 1513583334112
},
{
"name": "My Plan 2",
"description": "",
"URI": "/op/api/v1/firmwareupgradeplan/F44E875F-C7B5-4CC5-830B-0A9E39A005E5",
"lastUpdateTime": 1512052896724
}
]
}
```

Devices REST API

User will need an admin or operator access for this API, Unauthorized users will get "401 Unauthorized"

Add and setup a device:

Omitted Boolean parameters are presumed to be false, it's not allowed to setup wsm without setting up log targets
Omit the autoSetupAgentNameand autoSetupPattern parameters if you do not wish to use the automatic domain setup feature.

```
POST /op/api/v1/devices?name=wdp6&host=10.0.0.13&somaPort=5550&somaUser=admin&somaPassword=password&logTargetAddress=10.0.0.13&monitorResources=false&monitorServices=true&syslogAgentName=MonTier-SyslogAgent-1&setupSyslogForDomains=true&wsmAgentName=MonTier-WsmAgent-1&setupWsmForDomains=true&setupCertificateMonitor=true&autoSetupPattern=APIMgmt*&autoSetupAgentName=MonTier-SyslogAgent-1
{
"resultCode": "SUCCESS",
"resultMessage": ""
}
```

> **Error** messages are issued for input validation errors , errors while inserting the device into derby/es and errors that happened during the device-level syslog setup, when an error happens during those steps - the transaction is rolled-back and the device is removed from DPOD, so the command can be issued again without failing on a duplicate device error.
> **Warning** messages are issued for errors that happened while setting up log targets for all domains, setting up wsm for all domains or setting up certificate monitoring, the operation stops, but the transaction will not roll-back from DPOD, so manual steps will be needed in order to complete the setup.

Error - The operation either failed the input validation checks, or started but stopped, the device was rolled back from DPOD.

```
{
"resultCode": "ERROR",
"resultMessage": "A device with this name already exists, name=wdp6"
}
```

Warning - the operation started but stopped, we **did not** roll back the device or any setup done to this point, so the user will need to manually check what was setup and complete it manually.

```
{
"resultCode": "WARNING",
"resultMessage": "Error setting up WS-M agent for the following domains: Domain: APIMgmt_963162B289, Message: +DPOD WSM agent cannot be reached from the device. Error is: Cannot ping both host and IP address: TCP connection to \"10.0.0.38 port 60020\" failed (connection refused)"
}
```

Setup all devices' host aliases (for DR)

For all devices - disable all log targets, setup DPOD's host aliases again and re-enable all log targets.
If the device cannot be reached - it will be skipped.
Errors or exceptions will not stop the operation.

```
POST /op/api/v1/devices/refreshAgents
{
"resultCode": "SUCCESS"
}
```

Warning - not all the operations were completed for one or more devices, the operation completed successfully for devices that are not mentioned.

```
{
"resultCode": "WARNING",
"resultMessage": "Device=adp: Could not connect to device, skipping device, Exception=Could not connect to host. "
}
```

The operation does not return an "ERROR" status.

DevOps Portal REST API

Prerequisites

Requires admin or operator access, an operator user will also need specific user role that allows the operation (for example - validate remote WSDL)
Unauthorized requests will receive a "401 Unauthorized" response.

> The following API calls do NOT execute the operation, they just add it to the execution queue.
> The operation may not be executed at all (For example - the device was not accessible). you can view the operation result in the Services Portal Execution Status Page

Validate Remote WSDL

POST /op/api/v1/servicesportal/validateRemoteWsdl?deviceName=idg76_2&domainName=DMZ&serviceName=myServiceName&newRemoteWsdlAddress=http://new/wsdl/address

newRemoteWsdlAddress- optional parameter with the address of the new remote WSDL, you can omit this parameter to use the current address

Successful Response

```
{
"resultCode": "SUCCESS",
"resultMessage": "SUCCESS",
"executionId": 69,
"executionUUID": "E77225BB-7945-4E42-B1F6-041D1E109349"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultMessage": "There is already an in-progress action for this service, please wait until it is done."
}
```

Promote Remote WSDL

POST /op/api/v1/servicesportal/promoteRemoteWsdl?deviceName=idg76_2&domainName=DMZ&serviceName=myServiceName&newRemoteWsdlAddress=http://new/wsdl/address

newRemoteWsdlAddress- optional parameter with the address of the new remote WSDL, you can omit this parameter to use the current address

Successful Response

```
{
"resultCode": "SUCCESS",
"resultMessage": "SUCCESS",
"executionId": 69,
"executionUUID": "E77225BB-7945-4E42-B1F6-041D1E109349"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultMessage": "There is already an in-progress action for this service, please wait until it is done."
}
```

Validate Local WSDL

POST /op/api/v1/servicesportal/validateLocalWsdl?deviceName=idg76_2&domainName=DMZ&serviceName=myServiceName&filesPath=/myFolder/new&newWsdlFileName=myWsdl.svc.wsdl

filesPath - a folder that contains the WSDL and XSD files, it needs to be accessible to DPOD
newWsdlFileName - the name of the base WSDL file in the filesPath folder

Successful Response

```
{
"resultCode": "SUCCESS",
"resultMessage": "SUCCESS",
"executionId": 69,
"executionUUID": "E77225BB-7945-4E42-B1F6-041D1E109349"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultMessage": "New WSDL file with name=myWsdl.svc.wsdl was not found in /myFolder/new"
}
```

Promote Local WSDL

POST /op/api/v1/servicesportal/promoteLocalWsdl?deviceName=idg76_2&domainName=DMZ&serviceName=myServiceName&filesPath=/myFolder/new&newWsdlFileName=myWsdl.svc.wsdl

filesPath - a folder that contains the WSDL and XSD files, it needs to be accessible to DPOD
newWsdlFileName - the name of the base WSDL files in the filesPath folder

Successful Response

```
{
"resultCode": "SUCCESS",
"resultMessage": "SUCCESS",
"executionId": 69,
"executionUUID": "E77225BB-7945-4E42-B1F6-041D1E109349"
}
```

Error Response

```
{
"resultCode": "ERROR",
"resultMessage": "New WSDL file with name=myWsdl.svc.wsdl was not found in /myFolder/new"
}
```

DR REST API

User will need an admin or operator access for this API, Unauthorized users will get "401 Unauthorized"

Make a DPOD device the standby installation:
After intalling DPOD, run the following API to make it the standby machine,
you only need to run this API once after installation.

```
POST /op/api/v1/dr/makeStandby
```

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Success"
}
```

ERROR:

```
{
"resultCode": "ERROR",
"resultErrorCode": "EXCEPTION_OCCURRED",
"resultMessage": " Exception occurred while running DR API, exception UUID=01eef1c2-c0f9-4a4f-818c-0127d9c89400"
}
```

Change a standby DPOD installation to active mode:
Change the DPOD standby installation to active, this will change DPOD's log targets and host aliases on all monitored devices to point to the standby machine

> This API call may take several minutes to complete

```
POST /op/api/v1/dr/standbyToActive
```

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Success"
}
```

ERROR (all devices that are not mentioned in the error message were setup successfully):

```
{
"resultCode": "ERROR",
"resultErrorCode": "ERROR_FROM_SETUP_SYSLOGS",
"resultMessage": " -- could not connect to device, deviceName=XG45-QA-101 deviceHost=192.168.72.50"
}
```

Change a standby DPOD installation back to inactive mode:

```
POST /op/api/v1/dr/standbyToInactive
```

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Success"
}
```

ERROR:

```
{
"resultCode": "ERROR",
"resultErrorCode": "ALREADY_IN_STANDBY_MODE",
"resultMessage": "DPOD is already in standby mode"
}
```

Change the active DPOD installation back to active mode:
Change the active DPOD installation to be active again after recovering from the DR situation, this will change DPOD's log targets and host aliases on all monitored devices to point to the active machine

> This API call may take several minutes to complete

POST /op/api/v1/dr/activeBackToActive

```
{
"resultCode": "SUCCESS",
"resultErrorCode": "SUCCESS",
"resultMessage": "Success"
}
```

ERROR (all devices that are not mentioned in the error message were setup successfully):

```
{
"resultCode": "ERROR",
"resultErrorCode": "ERROR_FROM_SETUP_SYSLOGS",
"resultMessage": " -- could not connect to device, deviceName=XG45-QA-101 deviceHost=192.168.72.50"
}
```

Reports REST API

User will need an opDashOperatorRole access for this API

Run report by reference:

```
GET /op/api/v1/reports/00000000-0000-0000-0000-a10000000001
```

```
{
  "executionID":51,
  "reportName":"Device CPU",
  "message":"Report Executed",
  "status":"OK"
}
```

Example of an error:

```
{
"summary":"Exception:Reference 2F522097-7F15-4C91-91C7-4B566ABA136X not found in Reports table
(org.montier.reports.rest.ReportResource.executeReport(ReportResource.java:59))",
"message":"Reference 2F522097-7F15-4C91-91C7-4B566ABA136X not found in Reports table",
"status":"error"
}
```

Get all available reports:

```
GET  /op/api/v1/reports/
```

The lastUpdateTime field returns the last time the alert was updated in epoch time format

```
{
"reports":[
{
"name":"Executed Transactions Report",
"description":"List of all executed transactions",
"URI":"/op/api/v1/reports/e123a124-647f-4de0-9b3e-71875e7eee90",
"lastUpdateTime":1529941818967
},
{
"name":"Device Resources Report",
"description":"All device resources samples",
"URI":"/op/api/v1/reports/65beb0d6-7f78-4b48-a6cb-cd21a7c3a983",
"lastUpdateTime":1529941818971
},
{
"name":"Message Codes Count Report",
"description":"Message codes distribution",
"URI":"/op/api/v1/reports/61e12f8f-97bc-4cd2-8fc3-b9c4dc9b0d8e",
"lastUpdateTime":1529941818976
},
{
"name":"Device CPU",
"description":"Devices ordered by average CPU",
"URI":"/op/api/v1/reports/2F522097-7F15-4C91-91C7-4B566ABA136F",
"lastUpdateTime":1529852908149
}
]
}
```

WS-M Subscription REST API

> User will need an opDashAdminRole access for this API.

CREATE A WS-M SUBSCRIPTION

POST /op/api/v1/wsmSubscriptions

Example of a request body:

Example of a successful response:

Gateway/s REST API

User will need an admin access for this API, Unauthorized users will get "401 Unauthorized"

Get Gateway By Name:

```
curl -X POST \
  https://<IP>:443/op/api/v1/gateways/getByName \
  -H 'Authorization: Basic YWRtaW46YWRtaW51c2Vy' \
  -H 'Cache-Control: no-cache' \
  -H 'Content-Type: application/json' \
  -H 'cache-control: no-cache' \
  -d '{
    "name": "datapower1-7dc474c48c-chtpg"
}'
```

Result example:

```
{
    "result": {
        "host": "172.17.100.100",
        "id": 103,
        "isDeviceResourcesMonitored": true,
        "isServiceResourcesMonitored": true,
        "logTargetSourceAddress": "192.168.226.229",
        "name": "datapower1-7dc474c48c-chtpg",
        "somaPort": 5550,
        "somaUserName": "admin"
    },
    "resultCode": "SUCCESS"
}
```

Update Gateway:

```
curl -X PUT \
  https://<IP>:443/op/api/v1/gateway/<ID> \
  -H 'Authorization: Basic YWRtaW46YWRtaW51c2Vy' \
  -H 'Content-Type: application/json' \
  -H 'cache-control: no-cache' \
  -d '{
    "name": "datapower1-7dc474c48c-chtpg",
    "host": "172.17.100.100",
    "somaPort": "5550",
    "somaUserName": "admin",
    "somaPassword": "admin",
    "logTargetSourceAddress": "192.168.226.229",
    "isDeviceResourcesMonitored": "true",
    "isServiceResourcesMonitored": "true",
    "reSetupSyslogForDevice": "true",
    "reSetupSyslogForAllDomains": "false",
    "reSetupWsmForDevice": "false",
    "reSetupWsmForAllDomains": "false"
}'
```

The following fields are mandatory: reSetupSyslogForDevice/reSetupSyslogForAllDomains/reSetupWsmForDevice/reSetupWsmForAllDomains

Result example:

```
{
   "result": {
        "id": 103
    },
  "resultCode": "SUCCESS"
}
```

Appliance Maintenance Status Codes

- Maintenance Plans Status Description
- Backup Tasks Status Codes
- Sync Tasks Status Codes
- Firmware Upgrade Status Codes

Maintenance Plans Status Description

Here are some common statuses for Backup and Sync plan executions,

Status Code	Description
WAITING_FOR_PRE_VALIDATION	The plan was entered into the execution queue, it was not yet validated or checked, and eventually may not get executed
BACKUPS_ARE_DISABLED	The plan will not execute - all backups were disabled (see Configurable Parameters and Settings)
SYNCS_ARE_DISABLED	The plan will not execute - all syncs were disabled (see Configurable Parameters and Settings)
PREPROCESS_EXECUTION_SKIPPED_BECAUSE_A_DAY_PASSED	The plan was waiting in the queue for a day or more and will be canceled, no tasks were executed yet.
PRE_VALIDATION_QUIESCE_TIMEOUT_SYSPARM_TOO_SHORT	The plan will not execute - the configured quiesce parameter (see Configurable Parameters and Settings) is shorter than 60 seconds
PRE_VALIDATION_OUT_OF_MAINTENANCE_WINDOW	The plan will not execute - the current time is not within the maintenance window (see Maintenance Concepts for more information about the maintenance window), the maintenance window is checked for all execution types - schedules, ad-hoc via the UI and via the REST API
PRE_VALIDATION_INVALID_TIMEFRAME_FORMAT	The plan will not execute - the maintenance window defined in system parameters is in an invalid format, the format should be HH:MM (see Configurable Parameters and Settings)
PRE_VALIDATION_STORE_IS_NOT_MOUNTED	The plan will not execute - for backup plans - the backup destination must be a mounted remote filesystem , you cannot backup to the local filesystem created during DPOD installation (see Configurable Parameters and Settings on how to change the destination)
PRE_VALIDATION_BACKUP_STORE_OUT_OF_SPACE	The plan will not execute - there is not enough space in the backup destination path (DPOD checks the free space percent on the mounted path, see Configurable Parameters and Settings on how to change the threshold)
PRE_VALIDATION_BACKUP_STORE_PATH_NOT_FOUND	The plan will not execute - the backup destination path was not found (see Configurable Parameters and Settings on how to change the destination)
PRE_VALIDATION_CHECK_IF_STORE_MOUNTED_SCRIPT_EXCEPTION PRE_VALIDATION_BACKUP_STORE_SPACE_CHECK_EXCEPTION PRE_VALIDATIONS_EXCEPTION	The plan will not execute - Internal exception occurred, see the accompanying error message for more details
NO_TASKS_CREATED	The plan will not execute - no tasks created, this can happen, if no devices or domains were matching the pattern in the activity, or if no devices were available. for example, the backup activity specified Device QA1 and domain Bank*, but no such domains exist on device QA1.
NO_ELIGIBLE_TASKS	The plan will not execute - some tasks were created, but all of them were skipped or failed validations. For example, secure backup task for a device that was not in DR mode
PRE_VALIDATIONS_STARTED STARTED_DIVIDING_TO_TASKS TASKS_VALIDATIONS_STARTED TASKS_VALIDATIONS_FINISHED	Interim statuses - only used as progress indication, the plan will usually not stay in this status for more than a few minutes.
READY_FOR_EXECUTION	Interim status - the plan passed all validation and has some tasks waiting for execution, it is queued and will be executed in the next minute, or is waiting for other plans to finish executing first.

PRE_PLAN_SCRIPT_STARTED	Interim status - the plan is waiting for the pre-plan script to finish execute
PRE_PLAN_SCRIPT_FAILED	The plan will not execute - the pre-plan script returned with a return code greater than 0
EXECUTING	Interim status - one or more tasks started executing
POST_PLAN_SCRIPT_STARTED	Interim status - the plan is waiting for the post-plan script to finish execute
POST_PLAN_SCRIPT_FAILED	The plan finished executing, but the post-plan script returned with a return code greater than 0
SUCCESS_WITH_SKIPPED_TASKS	All tasks either finished successfully one or more tasks skipped (for example, because the device was not available)
SUCCESS	All tasks finished successfully
FAILED	One or more tasks failed

Backup Tasks Status Codes

Here are some common statuses for Backup task executions.

Status Code	Description
WAITING_FOR_PRE_VALIDATION	The task was entered into the execution queue, it was not yet validated or checked, and eventually may not get executed
SKIPPED_APIC_DOMAIN	The task will not execute - cannot backup API Connect domain
SKIPPED_DEVICE_NOT_AVAILABLE	The task will not execute - the device was not available
SKIPPED_NO_DEVICES_MATCHING_PATTERN	The task will not execute - no devices were matching the device pattern requested in the activity
DEVICE_NOT_IN_DR_MODE	The task will not execute - Secure Backup requested, but the device was not in DR mode
NOT_ENOUGH_FREE_SPACE_ON_DEVICE	The task will not execute - There is not enough free space in the DataPower temp storage (see Configurable Parameters and Settings on how to change the check's threshold)
CERT_DOESNT_EXIST_ON_DEVICE	The task will not execute - The certificate specified for Secure Backup was not found on the device
SKIPPED_BECAUSE_ERROR_POLICY EXECUTION_CANCELED_BECAUSE_ERROR_POLICY	The task will not execute - Another task failed and specified Error Policy = Fail (See Maintenance Concepts to learn more about Error Policies)
PLAN_FAILED_PRE_SCRIPT	The task will not execute - the pre-plan script returned with a return code greater than 0
EXECUTION_CANCELED_BECAUSE_A_DAY_PASSED	The task was not executed - it was automatically canceled because more than 24 hours passed since it started to wait for execution
EXECUTION_CANCELED_BECAUSE_MAINTENANCE_WINDOW	The task was not executed - the current time is not within the maintenance window (see Maintenance Concepts for more information about the maintenance window), the maintenance window is checked for all execution types - schedules, ad-hoc via the UI and via the REST API
READY_FOR_EXECUTION	Interim status - the task passed all validation, it is queued and will be executed in the next minute, or is waiting for other tasks to finish executing first.
SENT_TO_MDB EXECUTION_STARTED EXECUTION_PRE_CHECKS_STARTED	Interim status - the task is executing

EXECUTION_PRE_CHECKS_FOUND_QUIESCED_DOMAIN_IN_DEVICE	Task failed - quiesce deice requested (for Secure Backup or Export all domains) but found a domain that was already quiesced
EXECUTION_PRE_CHECKS_DOMAIN_IS_ALREADY_QUIESCED	Task failed - quiesce domain requested but the domain was already quiesced
EXECUTION_PRE_CHECKS_NFS_OUT_OF_SPACE	Task failed - The specified backup destination is out of space, see Configurable Parameters and Settings on how to check this check threshold
EXECUTION_PRE_CHECKS_NFS_DIRECTORY_NOT_FOUND	Task failed - The specified backup destination was not found, see Configurable Parameters and Settings on how to change the destination
EXECUTION_PRE_CHECKS_DEVICE_NOT_AVAILABLE	Task failed - the DataPower device was not available
EXECUTION_CHECK_MANIFEST_WAITING_FOR_ANOTHER_BACKUP	The task is waiting for another DPOD backup task to finish running on the device
EXECUTION_CHECK_MANIFEST_ANOTHER_SECURE_BACKUP_IS_RUNNING_CHECK_DEVICE	Task failed - this may happen if DPOD was restarted while a backup task was running, it seems that the backup task is still executing, but DPOD lost track of it, check the device manually.
EXECUTION_WAITING_FOR_PRE_SCRIPT	Waiting for the user pre script to execute
EXECUTION_PRE_SCRIPT_ERROR	Task failed - the user pre task script return code was larger than 0, the post task script will still be executed (if specified)
EXECUTION_QUIESCE_STARTED	Quiesce domain/device started
EXECUTION_QUIESCE_WAITING_FOR_QUIESCE	Waiting for the device or domain to quiesce
EXECUTION_QUIESCE_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device or domain to quiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout)
EXECUTION_EXPORT_DOMAIN_PERSISTED_STARTED EXECUTION_EXPORT_DOMAIN_NON_PERSISTED_STARTED	Export-Domain started
EXECUTION_EXPORT_DOMAIN_PERSISTED_SOMA_ERROR EXECUTION_EXPORT_DOMAIN_NON_PERSISTED_SOMA_ERROR	Error occurred in the Export-Domain process
EXECUTION_EXPORT_DOMAIN_PERSISTED_EMPTY_FILE EXECUTION_EXPORT_DOMAIN_NON_PERSISTED_EMPTY_FILE	The Export Domain process returned an empty file
EXECUTION_EXPORT_DOMAIN_PERSISTED_SAVEFILE_EXCEPTION EXECUTION_EXPORT_DOMAIN_NON_PERSISTED_SAVEFILE_EXCEPTION	An error occurred while saving the Export Domain zip file to DPOD
EXECUTION_EXPORT_DOMAIN_PERSISTED_DONE EXECUTION_EXPORT_DOMAIN_NON_PERSISTED_DONE	Export-Domain finished successfully
EXECUTION_SECURE_BACKUP_STARTED	Secure Backup started
EXECUTION_SECURE_BACKUP_UNSUCCESSFUL	Secure Backup returned an error

EXECUTION_SECURE_BACKUP_WRONG_FILE_HASH EXECUTION_SECURE_BACKUP_WRONG_FILE_SIZE EXECUTION_SECURE_BACKUP_EMPTY_FILE	Downloading the Secure Backup files from the DataPower temp folder to DPOD failed
EXECUTION_UNQUIESCE_STARTED EXECUTION_UNQUIESCE_ON_ERROR_STARTED	Unquiesce domain/device started
EXECUTION_UNQUIESCE_WAITING_FOR_UNQUIESCE EXECUTION_UNQUIESCE_ON_ERROR_WAITING_FOR_UNQUIESCE	Waiting for domain/device to unquiesce
EXECUTION_UNQUIESCE_TIMEOUT_OCCURRED EXECUTION_UNQUIESCE_ON_ERROR_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device or domain to unquiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout)
EXECUTION_FAILED_WITH_INTERNAL_EXCEPTION	Internal error occurred, see error message for details
EXECUTION_FAILED_LONG_RUNNING	The task was running for more than 60 minutes (see Configurable Parameters and Settings on how to change this duration) and was marked as finished, the task may still be executing, manual intervention may be required
FAILED_NO_FILES_DOWNLOADED	No errors occurred, but no files downloaded to DPOD - this may happen if DPOD was restarted during the backup process Try to run the backup again
SUCCESS	The backup finished successfully

Sync Tasks Status Codes

Status Code	Description
WAITING_FOR_PRE_VALIDATION	Task entered the execution queue, but has not yet been validated or checked, and eventually may not get executed
SKIPPED_APIC_DOMAIN	Task will not execute - cannot sync API Connect domain
SKIPPED_SOURCE_DEVICE_DOES_NOT_EXIST	Task will not execute - the source device specified in the activity does not exist
SKIPPED_SOURCE_DEVICE_NOT_AVAILABLE	Task will not execute - the source device was not available
SKIPPED_TARGET_DEVICE_DOES_NOT_EXIST	Task will not execute - the target device specified in the activity does not exist
SKIPPED_TARGET_DEVICE_NOT_AVAILABLE	Task will not execute - the target device was not available
SKIPPED_NO_DEVICES_MATCHING_PATTERN	Task will not execute - no devices matching the pattern specified in the activity were found
SKIPPED_NO_DOMAINS_FOUND_IN_SOURCE_DEVICE	Task will not execute - no domains matching the pattern specified in the activity were found
SKIPPED_DOMAIN_DOESNT_EXIST_IN_TARGET_DEVICE	Task will not execute - the specified domain exists in the source device but not in the target device DPOD does not create domains on the target devices, it is your responsibility to create them
SKIPPED_DOMAIN_WAS_NOT_CHANGED	Task will not execute - for scheduled plans, no changes were found in the source domain since the last time it was synced to the target domain
VALIDATION_STARTED VALIDATIONS_OK	Interim status - DPOD is validating the task
ERROR_DEVICE_FIRMWARE_NOT_SUPPORTED	Task will not execute - sync is supported only when the source and target devices' firmware level is higher or equal to 7.1.0.0
ERROR_DEVICE_TYPE_INCOMPATIBLE	Task will not execute - sync is possible only from lower to higher device type XG-45 < XI-52 < XB-62 < IDG You can turn this check off in the sync activity definition
ERROR_FIRMWARE_LEVELS_INCOMPATIBLE	Task will not execute - sync is possible only from lower major firmware level to an equal or higher firmware level (e.g. 7.2.0.X to 7.2.0.X and higher) You can turn this check off in the sync activity definition
ERROR_TARGET_MISSING_FEATURES	Task will not execute - the target device is missing features/licenses found in the source device (e.g. B2B, SQL-ODBC, Tibco-ESM) You can turn this check off in the sync activity definition

ERROR_UNSUPPORTED_DEVICE_TYPE	Task will not execute - only the following device types are supported: IDG, XB-62, XI-52, XG-45
ERROR_DEPLOYMENT_POLICY_WAS_NOT_FOUND_IN_SOURCE_DOMAIN	Task will not execute - the deployment policy specified in the sync activity definition was not found in the source domain
ERROR_DEPLOYMENT_POLICY_WAS_NOT_FOUND_IN_TARGET_DOMAIN	Task will not execute - the deployment policy specified in the sync activity definition was not found in the target domain
ERROR_DEPLOYMENT_POLICY_VARIABLES_WAS_NOT_FOUND_IN_TARGET_DOMAIN	Task will not execute - the deployment policy variables object specified in the sync activity definition was not found in the target domain
ERROR_NEEDS_USER_APPROVAL_TO_CREATE_TEST_OBJECTS	Task will not execute - for firmware levels above 7.5.2.4, DPOD will try to check if the passphrase is identical in source and target devices, in order to perform this check, DPOD will need to create a temporary password map object in the source domain, you will need to approve this object creation in the sync activity definition
ERROR_SOURCE_AND_TARGET_PASSPHRASE_ARE_DIFFERENT	Task will not execute - the source and target passphrases are different
PLAN_FAILED_PRE_SCRIPT	Task will not execute - the pre-plan script returned with a return code greater than 0
SKIPPED_BECAUSE_ERROR_POLICY EXECUTION_CANCELED_BECAUSE_ERROR_POLICY	Task will not execute - Another task failed and specified Error Policy = Fail (See Maintenance Concepts to learn more about Error Policies)
READY_FOR_EXECUTION	Interim status - the task passed all validation, it is queued and will be executed in the next minute, or is waiting for other tasks to finish executing first.
WAITING_FOR_EXPORT_TASK	Interim status - the import task to the target domain is waiting for the export task from the source domain to finish executing
ALL_DEPENDENT_IMPORT_TASKS_SKIPPED	The export task was skipped - no import tasks are waiting for the export (for example, because the target devices were not available)
EXECUTION_CANCELED_BECAUSE_MAINTENANCE_WINDOW	Task was not executed - the current time is not within the maintenance window (see Maintenance Concepts for more information about the maintenance window), the maintenance window is checked for all execution types: schedules, ad-hoc via the UI and via the REST API
SENT_TO_MDB EXECUTION_STARTED EXECUTION_PRE_CHECKS_STARTED	Interim status - the task is executing
EXECUTION_PRE_CHECKS_DOMAIN_IS_ALREADY_QUIESCED	Task failed - quiesce domain requested but the domain was already quiesced
EXECUTION_PRE_CHECKS_DEVICE_NOT_AVAILABLE	Task failed - the DataPower device was not available
EXECUTION_WAITING_FOR_PRE_SCRIPT	Waiting for the user pre-script to execute
EXECUTION_PRE_SCRIPT_ERROR	Task failed - the user pre task script return code was larger than 0, the post task script will still be executed (if specified)

EXECUTION_EXPORT_DOMAIN_STARTED	Interim status - exporting data from the source domain
EXECUTION_EXPORT_DOMAIN_SOMA_ERROR	Task failed - the export domain process returned an error
EXECUTION_EXPORT_DOMAIN_RETURNED_EMPTY_FILE	Task failed - the export domain process returned an empty export file
EXECUTION_QUIESCE_STARTED	Quiesce domain/device started
EXECUTION_QUIESCE_WAITING_FOR_QUIESCE	Waiting for the device or domain to quiesce
EXECUTION_QUIESCE_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device or domain to quiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout)
EXECUTION_IMPORT_DOMAIN_DRY_RUN_STARTED	Interim status - importing into the target domain started, this is a dry-run import and WILL NOT change any data in the target domain.
EXECUTION_IMPORT_DOMAIN_DRY_RUN_UNSUCCESSFUL	Task failed - the import dry run returned an error
EXECUTION_IMPORT_DELETE_TARGET_OBJECTS_STARTED	Interim status - DPOD started to delete objects from the target domain
EXECUTION_IMPORT_DELETE_TARGET_OBJECTS_SOMA_ERROR	Task failed - the delete objects process returned an error
EXECUTION_IMPORT_DELETE_TARGET_OBJECTS_UNSUCCESSFUL	Task failed - could not delete one or more objects from the target domain
EXECUTION_IMPORT_DOMAIN_STARTED	Interim status - importing configuration to the target domain started
EXECUTION_IMPORT_DOMAIN_SOMA_ERROR EXECUTION_IMPORT_DOMAIN_EXCEPTION	Task failed - the import process returned an error NOTE: the target domain's objects were deleted, DPOD does not restore the domain to its previous state This error may indicate that the target device is under heavy load and cannot handle the import process, if no transactions are running on the device, this may happen when multiple sync tasks are running in parallel. Try to disable the "run in parallel" option in the sync plan or try again later
EXECUTION_IMPORT_DOMAIN_SAVE_CONFIG_UNSUCCESSFUL EXECUTION_IMPORT_DOMAIN_SAVE_CONFIG_EXCEPTION	Task failed - the domain may or may not have been synced, DPOD could not issue Save Configuration on the target device.Check the target domain status manually and save the configuration manually.
EXECUTION_UNQUIESCE_STARTED EXECUTION_UNQUIESCE_ON_ERROR_STARTED	Unquiesce domain/device started

EXECUTION_UNQUIESCE_WAITING_FOR_UNQUIESCE EXECUTION_UNQUIESCE_ON_ERROR_WAITING_FOR_UNQUIESCE	Waiting for domain/device to unquiesce
EXECUTION_UNQUIESCE_TIMEOUT_OCCURRED EXECUTION_UNQUIESCE_ON_ERROR_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device or domain to unquiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout)
EXECUTION_WAITING_FOR_POST_SCRIPT	Waiting for the user post script to execute
EXECUTION_POST_SCRIPT_ERROR	Task failed - the user post script return code was great than 0
SKIPPED_EXPORT_TASK_FAILED	(For Import tasks) Task skipped - the export source domain task failed, cannot perform the import task
EXECUTION_CANCELED_BECAUSE_A_DAY_PASSED	Task was not executed - it was automatically cancelled because more than 24 hours passed since it started to wait for execution
EXECUTION_FAILED_WITH_INTERNAL_EXCEPTION	Internal error occurred, see error message for details
EXECUTION_FAILED_LONG_RUNNING	The task was running for more than 60 minutes (see Configurable Parameters and Settings on how to change this duration) and was marked as finished, the task may still be executing, manual intervention may be required
SUCCESS	The export or import finished successfully

Firmware Upgrade Status Codes

Here are some common statuses for Firmware upgrade task executions.

Status Code	Description
WAITING_FOR_PRE_VALIDATION	The task was entered into the execution queue, it was not yet validated or checked, and eventually may not get executed
SKIPPED_DEVICE_DOES_NOT_EXIST SKIPPED_DEVICE_NOT_AVAILABLE	The task will not execute - the device was not available or does not exist/setup in DPOD
SKIPPED_NO_DEVICES_MATCHING_PATTERN	The task will not execute - no devices were matching the device pattern requested in the activity
VALIDATION_INTERNAL_EXCEPTION SKIPPED_INTERNAL_EXCEPTION ERROR_EXCEPTION_IN_PRE_VALIDATIONS	The task will not execute - an internal error occurred, a UUID will be printed, search the logs for this UUID in order to get more information
ERROR_IMAGE_FILE_DOES_NOT_EXIST	The task will not execute - The firmware image file that was specified for the activity was not found on disk see Configurable Parameters and Settings on how to change the image repository path
ERROR_UNSUPPORTED_DEVICE_TYPE	The task will not execute - The only supported device types are IDG, XB62, XI52 and XG45
ERROR_COULD_NOT_PARSE_IMAGE_FILE_NAME	The task will not execute - the image file's name was not in the standard format: modelType+firmwareVersion+.+features+.+imageFormat For example: idg7519.oradco.scrypt4
ERROR_DEVICE_AND_IMAGE_MODEL_GROUPS_ARE_DIFFERENT	The task will not execute - the image file's prefix indicated a model type different than the device type, For example, the image file was idg7519.oradco.scrypt4 but the device was XG45
ERROR_DOWNGRADE_NOT_SUPPORTED	The task will not execute - the firmware version of the image file was lower than the device's firmware version. Downgrade is supported only within the same major version (e.g. 7.5.1.7 to 7.5.1.4), only if approved in the activity definition
ERROR_DOWNGRADE_MAJOR_RELEASE_NOT_APPROVED	The task will not execute - the firmware version of the image file was lower than the device's version, but in the same major version (e.g. 7.5.1.7 to 7.5.1.4), User approval for the downgrade was not given in the activity definition
ERROR_DEVICE_AND_IMAGE_VERSIONS_ARE_IDENTICAL	The task will not execute - the firmware version of the image file was identical to the device's version.
ERROR_DEVICE_FEATURES_NOT_FOUND_IN_IMAGE	The task will not execute - the image file does not contain features (Tibco-EMS or DCO-Oracle) that found on the device The upgrade may still commence if user approval for this situation was given in the activity definition
ERROR_IMAGE_FEATURES_NOT_FOUND_IN_DEVICE	The task will not execute - the device does not contain features (Tibco-EMS or DCO-Oracle) that found in the image file
ERROR_UNKNOWN_IMAGE_FILE_FORMAT	The task will not execute - only image files that end with scrypt3 or scrypt4 are supported
ERROR_IMAGE_NOT_DESIGNED_FOR_VIRTUAL_DEVICES	The task will not execute - scrypt3 file was chosen for upgrading virtual appliance
ERROR_IMAGE_NOT_DESIGNED_FOR_PHYSICAL_DEVICES	The task will not execute - scrypt4 file was chosen for upgrading physical appliance
ERROR_NOT_ENOUGH_FREE_ENCRYPTED_SPACE_ON_DEVICE	The task will not execute - there is not enough free space to upload the image file to the device's encrypted file system (free space is needed in both encrypted and temporary file systems)

ERROR_NOT_ENOUGH_FREE_TEMP_SPACE_ON_DEVICE	The task will not execute - there is not enough free space to upload the image file to the device's temporary file system (free space is needed in both encrypted and temporary file systems)
ERROR_FOUND_UNSAVED_CHANGES_ON_DEVICE	The task will not execute - Unsaved changes were found in the device, apply all unsaved changes before starting the firmware upgrade again.
SKIPPED_BECAUSE_ERROR_POLICY EXECUTION_CANCELED_BECAUSE_ERROR_POLICY	The task will not execute - Another task failed and specified Error Policy = Fail (See Maintenance Concepts to learn more about Error Policies)
ERROR_WHILE_GETTING_DEVICE_LICENSES ERROR_GETTING_SOURCE_DOMAIN_STATUS ERROR_EXCEPTION_WHILE_GETTING_SOURCE_DOMAIN_STATUS	The task will not execute - and error was returned when DPOD was communicating with the monitored device. Search the log files with the error code for more information.
PLAN_FAILED_PRE_SCRIPT	The task will not execute - the pre-plan script returned with a return code greater than 0
EXECUTION_CANCELED_BECAUSE_A_DAY_PASSED	The task was not executed - it was automatically canceled because more than 24 hours passed since it started to wait for execution
EXECUTION_CANCELED_BECAUSE_MAINTENANCE_WINDOW	The task was not executed - the current time is not within the maintenance window (see Maintenance Concepts for more information about the maintenance window), the maintenance window is checked for all execution types - schedules, ad-hoc via the UI and via the REST API
READY_FOR_EXECUTION	Interim status - the task passed all validation, it is queued and will be executed in the next minute, or is waiting for other tasks to finish executing first.
SENT_TO_MDB EXECUTION_STARTED EXECUTION_PRE_CHECKS_STARTED	Interim status - the task is executing
EXECUTION_PRE_CHECKS_FOUND_QUIESCED_DOMAIN_IN_DEVICE	Task failed - one or more domains are quiesced, unquiesce all domains before running the upgrade
EXECUTION_PRE_CHECKS_DEVICE_FIRMWARE_LEVEL_CHANGED	Task failed - The firmware level of the device was changed by an external party during the upgrade task execution, DPOD will assume that another upgrade (manual or by DPOD) is running and will stop the execution
EXECUTION_PRE_CHECKS_DEVICE_NOT_FOUND EXECUTION_PRE_CHECKS_DEVICE_NOT_AVAILABLE	Task failed - the DataPower device was not available, or not found in DPOD managed devices.
EXECUTION_WAITING_FOR_PRE_SCRIPT	Waiting for the user pre script to execute
EXECUTION_PRE_SCRIPT_ERROR	Task failed - the user pre task script return code was larger than 0, the post task script will still be executed (if specified)
EXECUTION_FIRST_QUIESCE_STARTED EXECUTION_SECOND_QUIESCE_STARTED	Quiesce domain/device started First Quiesce = optional quiesce that can be requested by the user Second Quiesce = a mandatory quiesce that is issued by DPOD just before the upgrade starts
EXECUTION_FIRST_QUIESCE_WAITING_FOR_QUIESCE EXECUTION_SECOND_QUIESCE_WAITING_FOR_QUIESCE	Waiting for the device or domain to quiesce First Quiesce = optional quiesce that can be requested by the user Second Quiesce = a mandatory quiesce that is issued by DPOD just before the upgrade starts

EXECUTION_FIRST_QUIESCE_TIMEOUT_OCCURRED EXECUTION_SECOND_QUIESCE_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device or domain to quiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout) First Quiesce = optional quiesce that can be requested by the user Second Quiesce = a mandatory quiesce that is issued by DPOD just before the upgrade starts
EXECUTION_RESTART_TIMEOUT_OCCURRED	A timeout occurred while waiting for the device to restart, the timeout can be configured - see Configurable Parameters and Settings DPOD stops the operation and will not upgrade the device
EXECUTION_RESTART_WAITING_FOR_RESTART	DPOD is waiting for the device to restart
EXECUTION_WAIT_AFTER_RESTART_STARTED	DPOD is waiting for the time specified in the activity definition (this can only happen after a restart was completed successfully)
EXECUTION_UPLOAD_IMAGE_STARTED EXECUTION_WAITING_FOR_UPLOAD_IMAGE	DPOD is uploading the image file to the device
EXECUTION_UPLOAD_IMAGE_ERROR	Task failed - error occurred while uploading the image file to the device, DPOD uses a script to upload the file - search the logs for "EXECUTION_UPLOAD_IMAGE_ERROR" to see the detailed output the script.
EXECUTION_UPGRADE_STARTED	DPOD started the firmware upgrade on the monitored device.
EXECUTION_UPGRADE_WAITING_FOR_UPGRADE	The upgrade was started, the device will restart during the process, DPOD is waiting for the device to finish the upgrade
EXECUTION_UPGRADE_TIMEOUT_OCCURRED	Task failed - DPOD waited for the device to upgrade more than the time that was specified in the activity definition The device may or may not have been successfully upgraded, you should check the device's status manually
EXECUTION_UNQUIESCE_ON_ERROR_STARTED	An error occured in a previous state while the device was quiesced, DPOD is unquiescing the device before ending the task
EXECUTION_UNQUIESCE_ON_ERROR_WAITING_FOR_UNQUIESCE	An error occured in a previous state while the device was quiesced, DPOD is unquiescing the device before ending the task
EXECUTION_UNQUIESCE_ON_ERROR_TIMEOUT_OCCURRED	An error occured in a previous state while the device was quiesced, DPOD tryed to unquiesce the device before ending the task, but aa timeout occurred while waiting for the device to unquiesce, the timeout can be configured - see Configurable Parameters and Settings (DPOD will add 3 minutes to the specified timeout)
EXECUTION_UPLOAD_IMAGE_EXCEPTION EXECUTION_UPGRADE_EXCEPTION_OCCURRED EXECUTION_SECOND_QUIESCE_EXCEPTION_OCCURRED EXECUTION_UNQUIESCE_ON_ERROR_EXCEPTION_OCCURRED	An internal error occurred, a UUID will be printed, search the logs for this UUID in order to get more information
EXECUTION_FAILED_WITH_INTERNAL_EXCEPTION	Internal error occurred, see error message for details
EXECUTION_FAILED_LONG_RUNNING	The task was running for more than 60 minutes (see Configurable Parameters and Settings on how to change this duration) and was marked as finished, the task may still be executing, manual intervention may be required
SUCCESS	The upgrade finished successfully

DevOps Services Portal's User Scripts

- Import Service User Scripts
- Local WSDL Validation and Promotion User Scripts

Import Service User Scripts

The DevOps Services Portal's import service action require two python scripts to run.

The first script returns the deployment policy that will be used for the import (it gets the user selected deployment policy and may override it)
The second script analyzes and validate the import file - for example, checks that it does not include a domain export

You may download and customize the sample scripts from https://bitbucket.org/montier/servicesportalscripts/src
If you wish to develop your own scripts, or customize the sample scripts, please follow the following guidelines.

Run Python -V from ssh to determine the Python version that comes with your DPOD installation.

FOLDER STRUCTURE

Each import execution receives a unique UUID - you can view the UUID in the DevOps Action Executions Status Page
Before each execution, DPOD creates a folder that will hold all files for this execution. the scripts are executed from this folder.
The default folder path (**basePath)** is /app/tmp/servicesportal/import/<uuid>
All execution files and folders older than 7 days will be automatically deleted by DPOD

When importing a service into multiple domains/devices, DPOD will run a separate import action for each service, so the scripts will run multiple times, each time the current imported service parameters will be passed and a new folder structure will be created.

DEPLOYMENT POLICY SELECTOR SCRIPT

Input Parameters:

1. Device Name of the target
2. Domain Name of the target
3. Service Name
4. Object Class (MPGW, XMLFW)
5. Executing User Name
6. Execution Source (UI or REST)
7. Execution UUID
8. The deployment policy file name that was selected by the user (without the path), or the value "noPolicy" if no policy was selected
9. The path where all policy files are stored (you may change this path from system parameters)

Output:

1. For the import process to continue, the script must end with RC=0, in this case, DPOD will use the deployment policy content that was written to the file "deployment-policy.txt"
   The deployment policy should contain the XML path /configuration/ConfigDeploymentPolicy (check out the sample script for an example on how to extract it):,
   for example:

2. If the script returns an RC > 0, DPOD's processing will stop, and an error message will be displayed, the error message will be the content of the file "deployment-policy.txt"

Sample Flow:

1. If the user selected deployment policy name X and the service name is Y - leave the deployment policy name as it is
2. If the user selected deployment policy name Z and the service name is Q or the Device Name is T - change the deployment policy name to V...
3. Next, if the deployment policy's extension is ZIP - extract it to a temp folder (and use /deppolicy/export.xml as the deployment policy file name)
4. Read the file as an XML tree
5. Run some validations on the XML - check that there is only one deployment policy element in the XML
6. Read the inner XML part of /configuration/ConfigDeploymentPolicy and write it to "deployment-policy.txt" for DPOD to use
7. Return with RC=0

IMPORT FILE VALIDATION SCRIPT

Input Parameters:

1. Import File Name
2. Import File Format (ZIP, XML, XCFG)
3. Device Name of the target
4. Domain Name of the target

5. Service Name
6. Object Class (MPGW, XMLFW)
7. Executing User Name
8. Execution Source (UI or REST)
9. Execution UUID
10. The deployment policy file name that was selected by the user, or the value "noPolicy" if none was selected, the deployment policy may have been overridden by the deployment policy selector script, you can read its content from deployment-policy.txt
    Note: Changes made to deployment-policy.txt by this validator script will not be reflected.

Output:

1. For the import process to continue - the script must end with RC=0
2. If the script ends with RC>0, the import will stop, any error messages written to the file "validation-output.txt" will be shown in the web console and the logs

Sample Flow:

1. if the file is a ZIP file - extract it
2. Make sure the "export.xml" file exists - if not, end with an error (write and error message to the file "validation-output.txt" and end with RC=1)
3. Read the export.xml file as XML tree
4. Make sure there is no /domains element (and if there is - end with error, domain export is not allowed)
5. Make sure there is only one service's configuration in the export file
6. Search the XML tree for /configuration/objectClass[@name=serviceName] - to make sure the file contains an export for the selected service - if not, end with error
7. Exit with RC=0

Local WSDL Validation and Promotion User Scripts

The DevOps Services Portal's Validate/Promote Local WSDL actions require two python scripts to run.

The first script analyzes the WSDL and retrieves all the referenced XSD, so DPOD can download them from the DataPower.
The second script analyzes the original WSDL and XSD files retrieved by the first script, and replaces all schema references in the new WSDL/XSD files that were uploaded by the user.
(Later on, DPOD will upload the new files to the DataPower)

You may download and customize the sample scripts from https://bitbucket.org/montier/servicesportalscripts/src
If you wish to develop your own scripts, or customize the sample scripts, please follow the following guidelines.

> Run Python -V from ssh to determine the Python version that comes with your DPOD installation.

FOLDER STRUCTURE

Each validate/promote execution receives a unique UUID - you can view the UUID in the DevOps Action Executions Status Page
Before each execution of Local WSDL validation/promotion, DPOD creates a folder that will hold all files for this execution.
The default folder path (**basePath)** is /app/tmp/servicesportal/wsdl/<uuid>
All execution files and folders older than 7 days will be automatically deleted by DPOD

ANALYZE SCRIPT

General Flow

1. DPOD will first call the analyze script with the current base WSDL as an input
2. The script will return all the XSD files referenced by the WSDL.
   If the WSDL doesn't reference any other schema files - the script will signal that no files are required and the flow will end.
3. DPOD will download the requested XSD files.
4. DPDO will run the script again to analyze the base WSDL and the downloaded XSD files and determine if more files should be downloaded.
   if more files are required - go to step 3 again.
   Otherwise - the flow ends.

Input

DPOD will pass the following data to the script

under **basePath/input.props** - input parameters passed from DPOD to the script (see below)
under **basePath/original/* -** in the first execution - the folder will contain the base WSDL of the service, in subsequent calls - the base WSDL of the service and any other XSD files that the previous script executions requested DPOD to download
under **basePath/logs/*** - backup of previous runs input.props files and any logs written by previous scripts

The input.props file passed from DPOD contains the following parameters:

call_timestamp - The timestamp when the script was called
calling_user_name - the DPOD user name that requested the validate/promote action
device_name - The service's device name
domain_name - the service's domain name
invoke_type - "UI" or "REST"
iteration - the iteration number - how many times the script was called before, the first iteration is 1.
log_files_path - the path where the script should write its logs if required
original_files_path - the path that contains the original WSDL/XSD files downloaded by DPOD
original_start_wsdl_dp_path - the DataPower's path of the current service WSDL
original_start_wsdl_name - the name that DPOD used to store the file containing the current service WSDL - the name may not be identical to the DataPower name, a number will be appended to it to avoid duplicate file names
request_uuid - the UUID of the execution
requested_operation - "validate" or "promote"
script_name - the script that was executed
service_name - the service name
total_original_schema_files - how many XSD files were downloaded in previous iterations (0 for the first call)

Example:

call_timestamp=1509552002476

```
calling_user_name=admin
device_name=idg76_2
domain_name=BankF_Domain
invoke_type=UI
iteration=1
log_files_path=/app/tmp/servicesportal/wsdl/9216E7A6-1408-494C-A580-A7F1A2B7BFEA/logs/
original_files_path=/app/tmp/servicesportal/wsdl/9216E7A6-1408-494C-A580-A7F1A2B7BFEA/original/
original_start_wsdl_dp_path=local:///AddCardToAccount_WHSW.wsdl
original_start_wsdl_name=AddCardToAccount_WHSW.wsdl-1
request_uuid=9216E7A6-1408-494C-A580-A7F1A2B7BFEA
requested_operation=promote
script_name=/app/custom/scripts/Download_wsdl_artifacts.py
service_name=AddCardToAccount_WHSW.WSP
total_original_schema_files=0
```

Output

DPOD expects the following completion code and output file :

Completion Code
0 - Success, the script terminated sucessfully, all WSDL and XSD files searched and DPOD doesn't need to download any more files
1 - Success, the scripts requests that DPOD will download files from the DataPower and will call it again.
99 - Error occured

Completion File
The script is required to write a file named completion-<iteration>.props to the **basePath** (the <iteration> is passed in the input.props file)
The file contents should include:

completion_code - the completion code (0 / 1 / 99)
error_message - error message if any, if there is no error message, leave the value empty
source_requesting_file.**X** - the full DataPower path and name of the file (WSDL or XSD) that included/imported the file to download (multiple entries)
file_to_download.**X** - the full DataPower path and name of the file (WSDL or XSD) that DPOD needs to download to the **basePath/original** folder (multiple entries)

Example:

```
completion_code=1
error_message=
source_requesting_file.0=local:///GPCalendarXML.svc.wsdl-1
file_to_download.0=local:///testService/GPCalendarXML.svc_wsdl0.wsdl
source_requesting_file.1=local:///GPCalendarXML.xsd-1
file_to_download.1=local:///testService/GPCalendarXML.xsd
```

REPLACE REFERENCES SCRIPT

General Flow

1. DPOD will execute the script only once
2. The script will change the new WSDL/XSD files that were uploaded by the user and replace all the references they contain to other XSD files

Input

under **basePath/input.props** - input parameters passed from DPOD to the script (see below).
under **basePath/original/* -** the original service files, downloaded previously by DPOD when executing the analyze script.
under **basePath/logs/*** - backup of previous runs' input.props files and any logs written by previous scripts.
under **basePath/new/*** - the new WSDL/XSD files the user uploaded.
under **basePath/altered/*** - an empty folder where the script should write the result WSDL/XSD files

The input.props file passed from DPOD contains the following parameters:

altered_files_path - where the script should write the final WSDL/XSD files with their references changes
call_timestamp - The timestamp when the script was called
calling_user_name - the DPOD user name that requested the validate/promote action
device_name - The service's device name
domain_name - the service's domain name
invoke_type - "UI" or "REST"
iteration - the iteration number - how many times the user scripts were called before (including the analyze script calls)
log_files_path - the path where the script should write its logs if required

new_files_path - the path where DPOD stored the new WSDL/XSD files that were uploaded by the user

new_schema_file.**X**.name - the name of the XSD file that was uploaded by the user (multiple entries)

new_start_wsdl_name - the name of the WSDL that was uploaded by the user

original_files_path - the path that contains the original WSDL/XSD files downloaded by DPOD

original_schema_file.**X**.dp_path - the datapower path of the current service XSD file (multiple entries)

original_schema_file.**X**.name - the name that DPOD used to store the file containing the current service XSD - the name may not be identical to the datapower name, a number will be appended to it to avoid duplicate file names

original_start_wsdl_dp_path - the datapower path of the current service WSDL

original_start_wsdl_name - the name that DPOD used to store the file containing the current service WSDL - the name may not be identical to the datapower name, a number will be appended to it to avoid duplicate file names

request_uuid - the UUID of the execution

requested_operation - "validate" or "promote"

script_name - the script that was executed

service_name - the service name

total_new_schema_files - how many new XSD files were uploaded by the user

total_original_schema_files - how many XSD files were downloaded in previous iterations

Example:

```
altered_files_path=/app/tmp/servicesportal/wsdl/39D54577-8D82-41BF-B497-81ACC068544C/altered/
call_timestamp=1508850533400
calling_user_name=admin
device_name=idg76_2
domain_name=DMZ
invoke_type=UI
iteration=4
log_files_path=/app/tmp/servicesportal/wsdl/39D54577-8D82-41BF-B497-81ACC068544C/logs/
new_files_path=/app/tmp/servicesportal/wsdl/39D54577-8D82-41BF-B497-81ACC068544C/new/
new_schema_file.0.name=GPCalendarXML.svc_wsdl0.wsdl
new_schema_file.1.name=GPCalendarXML.svc_xsd0.xsd
new_schema_file.2.name=GPCalendarXML.svc_xsd1.xsd
new_schema_file.3.name=GPCalendarXML.svc_xsd2.xsd
new_schema_file.4.name=GPCalendarXML.svc_xsd3.xsd
new_start_wsdl_name=GPCalendarXML.svc.wsdl
original_files_path=/app/tmp/servicesportal/wsdl/39D54577-8D82-41BF-B497-81ACC068544C/original/
original_schema_file.0.dp_path=local:///myService/GPCalendarXML.svc_wsdl0.wsdl
original_schema_file.0.name=GPCalendarXML.svc_wsdl0.wsdl-2
original_schema_file.1.dp_path=local:///myService/GPCalendarXML.svc_xsd0.xsd
original_schema_file.1.name=GPCalendarXML.svc_xsd0.xsd-3
original_schema_file.2.dp_path=local:///myService/GPCalendarXML.svc_xsd1.xsd
original_schema_file.2.name=GPCalendarXML.svc_xsd1.xsd-4
original_schema_file.3.dp_path=local:///myService/GPCalendarXML.svc_xsd2.xsd
original_schema_file.3.name=GPCalendarXML.svc_xsd2.xsd-5
original_schema_file.4.dp_path=local:///myService/GPCalendarXML.svc_xsd3.xsd
original_schema_file.4.name=GPCalendarXML.svc_xsd3.xsd-6
original_start_wsdl_dp_path=local:///myService/GPCalendarXML.svc.wsdl
original_start_wsdl_name=GPCalendarXML.svc.wsdl-1
request_uuid=39D54577-8D82-41BF-B497-81ACC068544C
requested_operation=promote
script_name=/app/custom/scripts/Replace_wsdl_references.py
service_name=assaflocal
total_new_schema_files=5
total_original_schema_files=5
```

Output

DPOD expects the following completion code and output file :

Completion Code
0 - Success, the script terminated succesfully, and wrote the altered files to the **basePath**/altered folder
99 - Error occured

Completion File
The script is required to create a file named completion-<iteration>.props to the **basePath** (the <iteration> is passed in the input.props file)
The file contents should include:

completion_code - the completion code (0 / 99)

error_message - error message if any, if there is no error message, leave the value empty

altered_wsdl_file.name - the local file name of the altered WSDL file

altered_wsdl_file.dp_path - the path+file name on the DataPower, DPOD will upload the file to this destination and will create any required directories.

altered_schema_file.**X**.name - the local file name of the altered XSD file (multiple entries)
altered_schema_file.**X**.dp_path - the path+file name on the DataPower, DPOD will upload the file to this destination and create any required directories. (multiple entries)

Example:

```
completion_code=0
error_message=
altered_wsdl_file.name=testWSDL.wsdl
altered_wsdl_file.dp_path=local:///817_testWSDL.wsdl
altered_schema_file.0.name=Service.asmx.xsd1.xsd
altered_schema_file.0.dp_path=local:///266_Service.asmx.xsd1.xsd
```

Integrations

- API Connect
- APM Integration
- Custom Transaction Log records

API Connect

To enable API Connect Integration with DPOD do as follow:

1. Check prerequisites : DPOD version v1.0.5+ and API Connect version v5.0.7.2 are required.
2. For DataPower FW 7.6 DPOD can monitor only one API Connect domain. This limitation should be removed in next firmware.
3. Setup log target from DPOD Web console for all DataPower Device, especially for API Connect domains.
4. You should consider enable the Auto Setup Domains feature that can create log target configuration automatically (as step 3) once new API Connect domain is created.
5. Once all this setup steps are completed, you should switch the transaction view to API Connect view
6. You can use the dedicated transaction list for API Connect.
7. You can also use APIs Availability dashboard to see last time an API invoked.

APM Integration

This is a tech preview feature

The Syslog record used is a JSON-formatted data object, containing information aggregated from several sources related to the transaction.When used, a Syslog record will be sent to an external APM (or any other Syslog server) for each gateway transaction.

The feature requires DataPower FW 7.6+.

Value to Customers

- This feature allows customers to easily display gateway information on their APMs or log aggregators such as IBM APM, Splunk or ELK. This isolates the customer from changes to DataPower's log structure and saves the need to parse Syslog records.
- Customers may link from the displayed transaction in their APM to DPOD's transaction details, in order to enhance troubleshooting efforts.
- DPOD customers can use this feature to externalize DPOD information for data warehouse purposes.
- DPOD customers can retain only the summarized transaction details instead of all log records. This will increase history retention time period and minimize storage requirements.

Transaction Record Structure

The following table describes the fields that are logged with this feature.

Field Name	Description	Possible Values
deviceName	DataPower gateway name	String
domainName	DataPower domain name where the transaction was executed	String
latencyElapsed	The elapsed time of the transaction in milliseconds	long
microSecTimestamp	Timestamp format of the time the transaction started	String
microSecTimestampStart	For internal use	String
microSecTimestampFinish	For internal use	String
serviceType	Service type as defined in the gateway	String - mpgw,wsp,xml-firewall,b2bgw
serviceUri	Request URI	String
serviceUrl	Request URL	String
srcNodeName	The name of the DPOD node that captured the transaction	String
isError	Indication whether the transaction completed with errors	Boolean true/false
isTechnicalError	Indication whether the transaction completed with errors	Boolean true/false
clientIp	The client IP of the machine (or load balancer) where the transaction started.	String
serviceName	The service the transaction ran on.	String
transactionId	DataPower transaction ID (TID)	String
transactionGlobalId	DataPower global transaction ID (GTID)	26 chars long
timeZone	The time zone used to log transaction start	String format +ZZ:ZZ
docAddedTimeInMil	For internal use	long
timeInMil	Transaction start time since Epoch in milliseconds	long number

timeHHMMSS	Full time of transaction start	String format HHMMSS where: HH: 00-23 MM: 00-59 SS: 00-59
requestSize	The request size	long
aggRecordVersion	Estimated FW version of the gateway that executed the transaction. (For internal use)	String

JSON Example

```
{
  "_index": "[logical-tran-compact_i3][0]",
  "_type": "wdpLogicalTransChild",
  "_id": "ea5ae3c55b45be5500056a13_348659",
  "_timestamp": "2018-07-11T08:22:45.457Z",
  "_version": 5,
  "_operation": "INDEX",
  "_source": {
    "deviceName": "1cb3a54303a9",
    "domainName": "Infra_Domain",
    "latencyElapsed": 2,
    "microSecTimestamp": "2018-07-11T11:22:45.313729+03:00",
    "microSecTimestampStart": "2018-07-11T11:22:45.313729+03:00",
    "microSecTimestampFinish": "2018-07-11T11:22:45.315558+03:00",
    "serviceType": "xmlfirewall",
    "serviceUri": "/UpdateWantedMenProfiles_WHSW/Service.asmx",
    "serviceUrl":
"http://Infra.HA:2555/UpdateWantedMenProfiles_WHSW/Service.asmx",
    "srcNodeName": "NODE0",
    "isError": false,
    "isTechnicalError": false,
    "clientIp": "172.77.77.5",
    "serviceName": "WSS_Loopback.XMLFW",
    "transactionId": "348659",
    "transactionGlobalId": "ea5ae3c55b45be5500056a13",
    "timeZone": "+03:00",
    "docAddedTimeInMil": 1531297365329,
    "timeHHMMSS": "11:22:45",
    "timeInMil": 1531297365313,
    "aggRecordVersion": "7.6.0.0+"
  }
}
```

Feature enablement

For each syslog agent in the system perform the following:

1. Edit the file /app/flume/syslog_agents/conf/MonTier-SyslogAgent-**nn**/flume_syslog.conf

2. Change the following property to **true** instead of **false**:
   MonTier-SyslogAgent-**nn**.sinks.syslogElasticSink**nnn**.serializer.enableLogicalTx = true

Stop and start Syslog agents

Custom Transaction Log records

1. Overview

The product has built-in capabilities based on the information it receives or samples from the monitored Gateways.

To enable the customer to send custom information to the product, the customer may modify their services and add a special transform action that will send additional information to the product that will be displayed within the product's console.

In the following paragraph you will find information on:

1. Describe the process of implementing the solution (modifying the services)
2. Describe the features that will be enabled by this solution
3. Describe the limitations of the solution

> **The nature of this solution is intrusive, as it requires manual modification of the customer services. The customer is responsible of modifying their services and testing them thoroughly before using the modified services.**

Customer that use this method usually have :

1. A single MPGW that execute dynamically based on the input the relevant internal flow. Such customer use this method to write the actual service name and other information available.
2. Other products that customer wishes to push their information into DPOD

DPOD v1.0.2+ includes a tech preview of this solution. The tech preview includes an ability to switch on (via a System Parameter) a new mode that uses the custom log records. Currently, only Transactions page and Service Activity dashboard are tuned to work with the new custom log records.

2. Implementing the Solution

2.1. The Need to Modify the Services

The product heavily relies on Syslog records sent by the Gateway to detect transactions and their attributes. To enable the customer to add custom information, the information must be provided as Syslog messages that are sent as part of the transaction. This can only be achieved by modifying the services, and manually adding a special transform action that will generate the required messages the product expects.

2.2. Syslog Record Format

The product is expecting a Syslog message in the following format and with specific log category and severity. See the XSLT template file for an example how to create such a Syslog message. Limitations of the Syslog message is documented under “Syslog Records Limitations”.

```
#^R2^A1:192.168.110.22^A2:Website User 123^A3:Loans^A4:Ping^A5:Approve^A6:0^A7:1^A8:1^A9:Backend returned HTTP 500^AA:Credit system request failed^AB:BCF345^AC:OK^AD:OK^AE:Ignored error^AF:1477802055111^AG:1477802066123^AH:100^AI:200^AJ:300^AK:400^AL:1000^AM:123^AN:456^AO:http://MNG:92/api/Approve.asmx^AP:192.168.1.85^AQ:chrome^AR:chrome-mobile^AS:111^AT:222^AU:333^AV:444^AW:555^AX:1.1^AY:2.2^AZ:3.3^B1:4.4^B2:5.5^B3:1^B4:0^B5:1^B6:0^B7:1^B8:Str1^B9:Str2^BA:Str3^BB:Str4^BC:Str5#^
```

2.3. XSLT File

2.3.1. CUSTOMIZING THE XSLT FILE

The customer will be provided with an XSLT template file that records all default information the product expects and creates the appropriate Syslog message. The customer may use it as an implementation reference. An additional XSLT file will be provided as a customization example. These XSLT files should be examined by the customer, modified as required and thoroughly tested before used.

The XSLT file contains placeholders for custom fields that the customer can set to override the default values the product collects. For example, while the product sets the Client IP field to the actual IP address the request was sent from, the customer may override this value in case an X-Forwarded-For header exists.

Custom fields in the XSLT have the notation: ***<!-- User code goes here -->***
All user code must be added only within these notations. For example, for the custom field "customServiceName":

2.3.2. LIST OF CUSTOM FIELDS IN XSLT

Field	Type	Description
customConsumer	String	A custom consumer name provided by the customer, based on the payload, headers, certificate etc.
customServiceName	String	A custom service name provided by the customer, based on the payload, headers or just to have meaningful service names.
customOperationName	String	A custom operation name provided by the customer, based on the payload, headers or just to have meaningful operation names.
isCustomError	0/1	Indicates whether the transaction was considered erroneous by the customer.
customErrorMessage	String	A custom error message provided by the customer. Trim this message after trimming technicalErrorMessage if total length of Syslog is still more than 1024 bytes. For future use.
customErrorCode	String	A custom error code provided by the customer. For future use.
customCompletionStatus	String	A custom completion status provided by the customer from the following list: STARTED, IN_PROGRESS, COMPLETED, ERROR, UNKNOWN, MISSING. For future use.
customCompletionReason	String	A custom completion reason in case completion status has been provided and more explanation is required. For future use.
customClientIp	String	A custom client IP provided by the customer (e.g. using X-Forwarded-For header).
customUserAgent	String	A custom user agent provided by the customer. For future use.
customNumber1-5	Number	For future use
customFloat1-5	Number	For future use
customBoolean1-5	0/1	For future use
customString1-5	String	For future use

2.3.3. USING CUSTOMIZED XSLT FILE

The customer may choose how to use the XSLT file after customizing it:

1. Upload the customized XSLT file to all Gateways monitored by the product. The customer may define the exact location and name of the XSLT file.
2. Copy the entire XSLT or parts of it, modify it, and use it within another XSLT they already have, as long as the generated Syslog message is in the same format the product is expecting. See an example of a Syslog message above and see the XSLT file for more information on how to create it.
3. There are 2 main implementation strategies.
    a. If the customer has main routing services, they can modify the routing services only. This will provide them information about all the transactions of the routing services. However, latency analysis and error analysis will be limited, since the product has no information about what happened in the services that were executed by the routing services.
    b. The customer may modify all their services. This will provide much more information to the product, but requires manual modification of all services.
4. A new transform action must be placed at the end of each relevant response rule, and each relevant error rule of a monitored service (may be implemented first on main routing services and if required on additional services later).
5. In case of a "One Way" service with no response rule, a new transform action must be placed at the end of the request rule.
6. If the new transform action is not located at the end of the processing rule, time measuring will be affected (see Transaction Times limitation below).

2.4. Modifying the Services

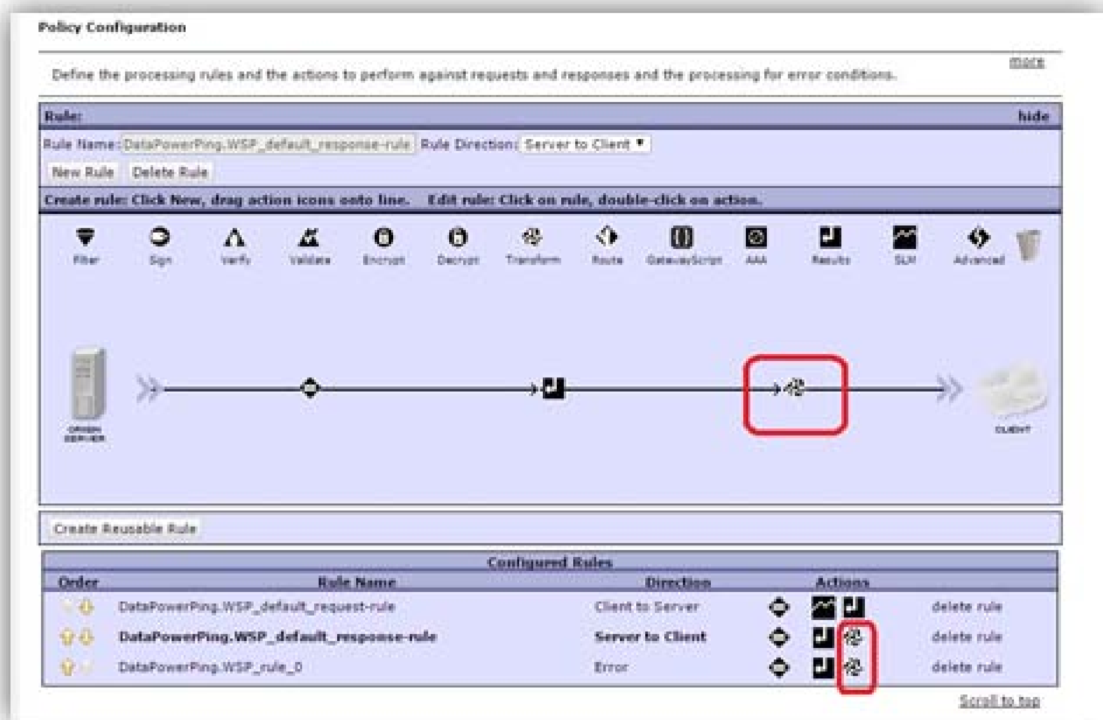
2.4.1. SUMMARY

1. There are 2 main implementation strategies.
    a. If the customer has main routing services, they can modify the routing services only. This will provide them information about all the transactions of the routing services. However, latency analysis and error analysis will be limited, since the product has no information about what happened in the services that were executed by the routing services.
    b. The customer may modify all their services. This will provide much more information to the product, but requires manual modification of all services.

2. A new transform action must be placed at the end of each relevant response rule, and each relevant error rule of a monitored service (may be implemented first on main routing services and if required on additional services later).
3. In case of a "One Way" service with no response rule, a new transform action must be placed at the end of the request rule.
4. If the new transform action is not located at the end of the processing rule, time measuring will be affected (see Transaction Times limitation below).

2.4.2. DETAILED EXPLANATION

1. Place a new transform action in the processing policy of the services you want to monitor. The transform action must be placed at the end of each relevant response rule, and each relevant error rule. In both cases, it should be placed after the result action, as the last action of the rule. The service must have both response and error rules.



Policy Configuration

Define the processing rules and the actions to perform against requests and responses and the processing for error conditions.

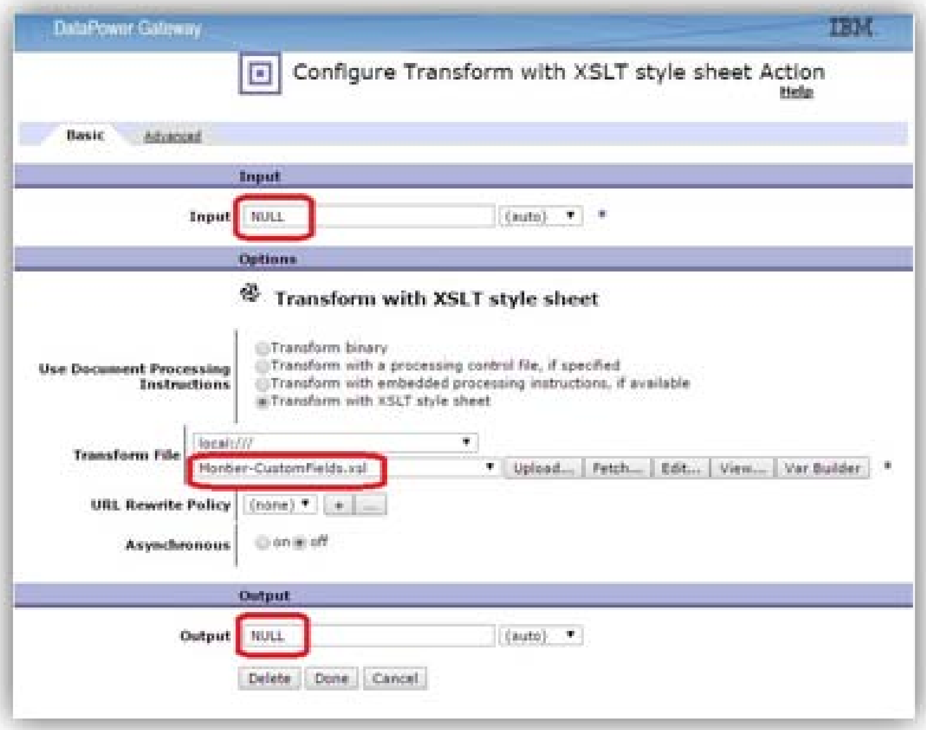
Rule:

Rule Name: DataPowerPing.WSP_default_response-rule Rule Direction: Server to Client

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Configured Rules			
Order	Rule Name	Direction	Actions
	DataPowerPing.WSP_default_request-rule	Client to Server	delete rule
	DataPowerPing.WSP_default_response-rule	**Server to Client**	delete rule
	DataPowerPing.WSP_rule_0	Error	delete rule

2. The transform action should use the XSLT file that was previously uploaded to the device or the customer's own XSLT that generates the Syslog message. The Input and Output of the transform action should both be NULL. The rest of the rule needs not be changed. The output of the result action will stay the same as it is.



Configure Transform with XSLT style sheet Action

Help

Basic | Advanced

Input

Input: NULL (auto) *

Options

Transform with XSLT style sheet

Use Document Processing Instructions:
○ Transform binary
○ Transform with a processing control file, if specified
○ Transform with embedded processing instructions, if available
● Transform with XSLT style sheet

Transform File: local:///
Monber-CustomFields.xsl *

URL Rewrite Policy: (none)

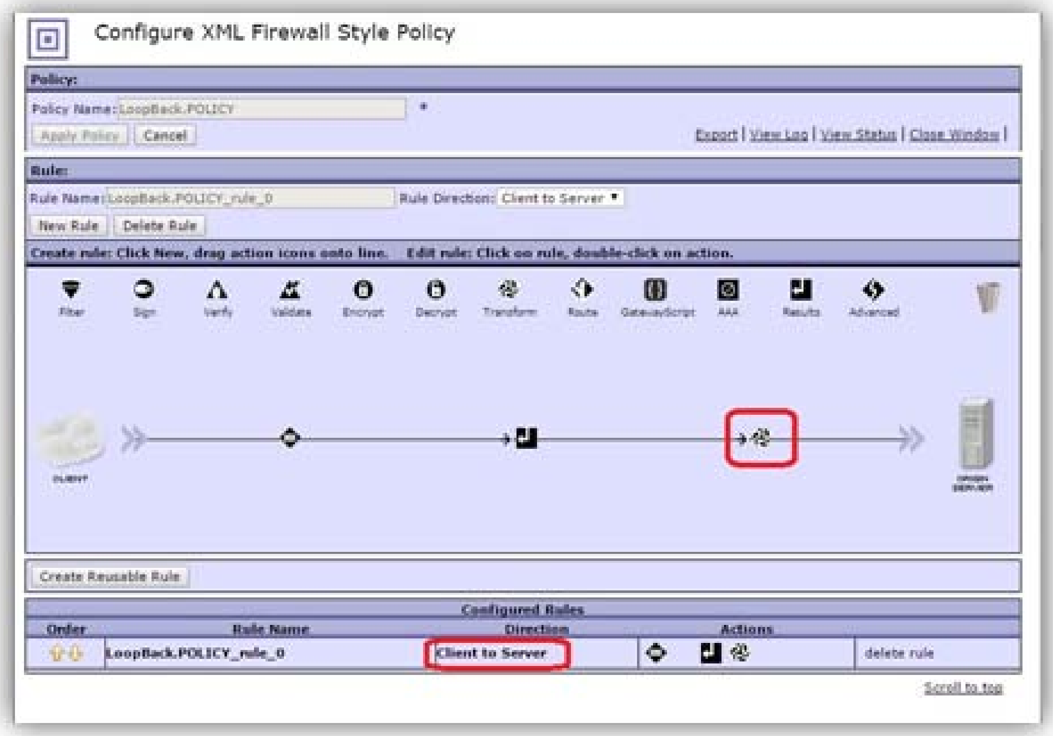
Asynchronous: ○ on ● off

Output

Output: NULL (auto)

3. In case of a "One Way" service, meaning that it has no response rule processing, the action must be placed at the end of the request rule.

In case of a loopback XMLFirewall:



Configure XML Firewall Style Policy

Policy:

Policy Name: LoopBack.POLICY *

Rule:

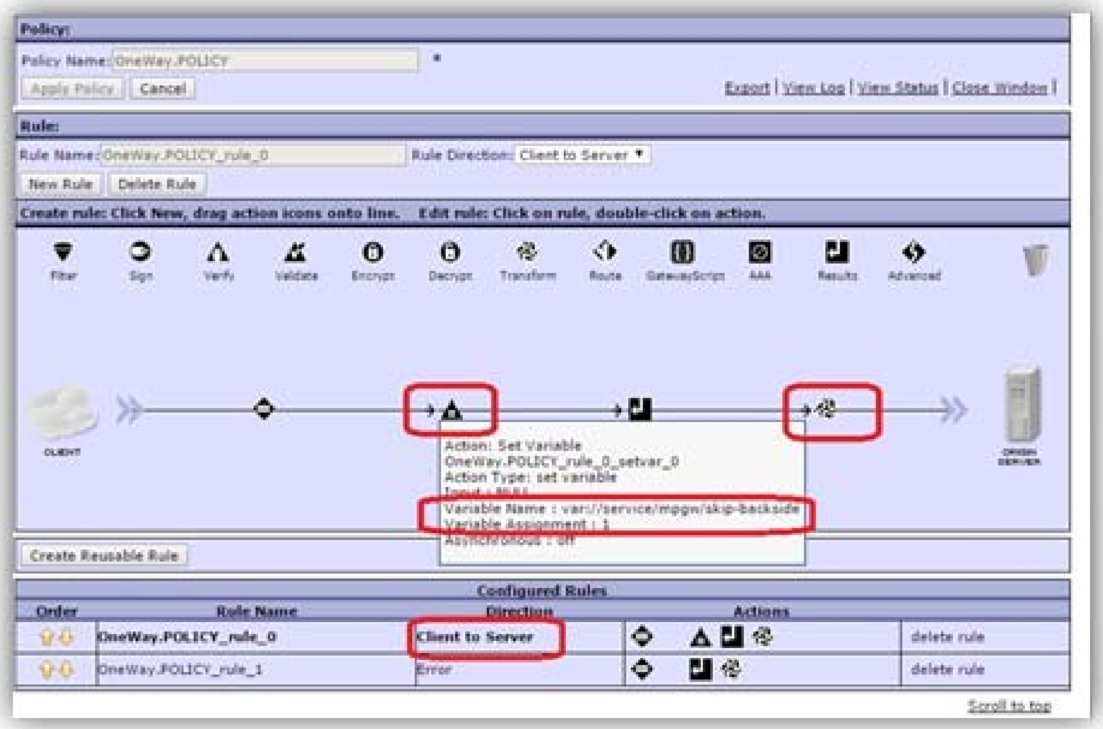
Rule Name: LoopBack.POLICY_rule_0 Rule Direction: Client to Server

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Configured Rules

Order	Rule Name	Direction	Actions	
	LoopBack.POLICY_rule_0	Client to Server		delete rule

In case of a Multi-Protocol Gateway or a Web-Service Proxy with the "var://service/mpgw/skip-backside" set to 1 (similar to a loopback behavior):



Policy Name: OneWay.POLICY *

Rule Name: OneWay.POLICY_rule_0 Rule Direction: Client to Server

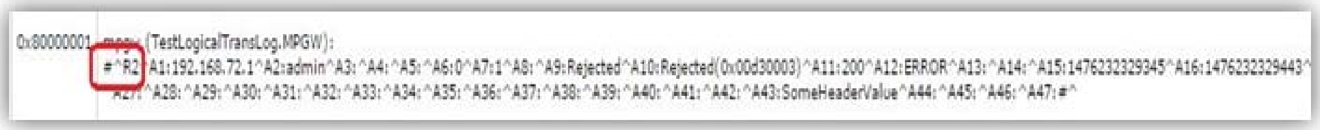
Action: Set Variable
OneWay.POLICY_rule_0_setvar_0
Action Type: set variable
Input : NULL
Variable Name : var://service/mpgw/skip-backside
Variable Assignment : 1
Asynchronous : off

Configured Rules

Order	Rule Name	Direction	Actions	
⇧⇩	**OneWay.POLICY_rule_0**	**Client to Server**		delete rule
⇧⇩	OneWay.POLICY_rule_1	Error		delete rule

2.5. Testing the Modified Services

Once the transform action is in place, the special Syslog messages can be viewed in the "view logs" window in the Gateway while transactions are processed. The messages can be recognized by the prefix "#^R2". For example:



```
0x80000001 mpgw (TestLogicalTransLog.MPGW):
#^R2^A1:192.168.72.1^A2:admin^A3:^A4:^A5:^A6:0^A7:1^A8:^A9:Rejected^A10:Rejected(0x00d30003)^A11:200^A12:ERROR^A13:^A14:^A15:1476232329345^A16:1476232329443^
A27:^A28:^A29:^A30:^A31:^A32:^A33:^A34:^A35:^A36:^A37:^A38:^A39:^A40:^A41:^A42:^A43:SomeHeaderValue^A44:^A45:^A46:^A47:#^
```

3. Features

The custom information that is provided by the customer is mostly used to be displayed when searching and investigating transactions. However, sometimes it is inevitable to display the technical information of the services. For example, in the Explore (service configuration) section, it only makes sense to display the name of the objects exactly as they are defined in the Gateway.

3.1. Existing Features

3.1.1. DASHBOARDS

All existing pages will be available. However, a few charts will not be displayed and some dashboards can only display technical information about services, as described in the Solution Limitations section below.

3.1.2. INVESTIGATE

All existing pages will be available. However, there are situations where technical information about services is displayed, as described in the Solution Limitations section below.

3.1.3. EXPLORE

All existing pages will be available. However, only technical information about the services is displayed because of the nature of this feature.

3.1.4. REPORTS

All out-of-the-box reports will be available. However, some reports will display technical information about the services, as described in the Solution Limitations section below.

4. Solution Limitations

4.1. Supported Services

The supported service types are:

1. Web-Service Proxy
2. Multi-Protocol Gateway
3. XML Firewall

Monitoring will only be available on modified services (that produces the new Syslog message).

Services that are **not** “One-Way” must have both response and error rules so the product can display both successful and failed transactions.

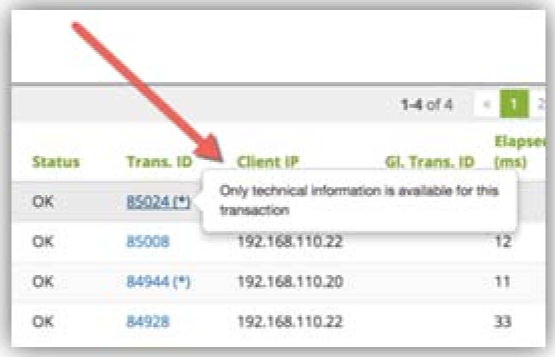
4.2. Features of Existing Version

4.2.1. DASHBOARDS

1. Service Latency: network latency charts (x4) will not be displayed.
2. Probes in Use: technical names of the services will be displayed.
3. Service Memory: technical names of the services will be displayed.
4. In case the customer uses the strategy of modifying only the routing services, the back-end analysis across the product will provide information about the services invoked by the routing services, and not the real back-end systems.
5. When searching within Payload, the search cannot be combined together with Status or Client IP filters. This is in addition to the Service filter, which is also not available in the current version of the product.
6. Since payload recording is enabled per domain, there could be a situation where the product receives payload information about transactions that belong to services that were not modified by the customer, and thus has no custom information about these transactions. In such a case, the product will display the technical information about the transaction and will mark the transaction ID with a special asterisk. Also, when displaying such a transaction in the Transaction page, only technical information will be displayed and a proper disclaimer will be used in the title next to the transaction number.
7. Extended Transaction feature is designed to work with the technical information of the transactions. If the customer is planning on using this feature, they would also need to customize the Extended Transaction XSLT files.

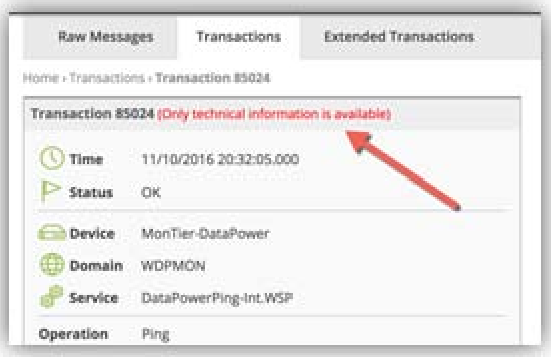
4.2.2. INVESTIGATE

1. In case the customer uses the strategy of modifying only the routing services, the back-end analysis across the product will provide information about the services invoked by the routing services, and not the real back-end systems.
2. When searching within Payload, the search cannot be combined together with Status or Client IP filters. This is in addition to the Service filter, which is also not available in the current version of the product.
3. Since payload recording is enabled per domain, there could be a situation where the product receives payload information about transactions that belong to services that were not modified by the customer, and thus has no custom information about these transactions. In such a case, the product will display the technical information about the transaction and will mark the transaction ID with a special asterisk. Also, when displaying such a transaction in the Transaction page, only technical information will be displayed and a proper disclaimer will be used in the title next to the transaction number.



Status	Trans. ID	Client IP	Gl. Trans. ID	Elapse (ms)
OK	85024 (*)			
OK	85008	192.168.110.22		12
OK	84944 (*)	192.168.110.20		11
OK	84928	192.168.110.22		33

Only technical information is available for this transaction



Transaction 85024 (Only technical information is available)

Time	11/10/2016 20:32:05.000
Status	OK
Device	MonTier-DataPower
Domain	WDPMON
Service	DataPowerPing-Int.WSP
Operation	Ping

4. Extended Transaction feature is designed to work with the technical information of the transactions. If the customer is planning on using this feature, they would also need to customize the Extended Transaction XSLT files.

4.2.3. REPORTS

- Service Memory: technical names of the services will be displayed.

4.3. Syslog Records

4.3.1. SYSLOG RECORD FORMAT

The product is expecting a Syslog message in a specific format and with specific log category and severity.

4.3.2. SYSLOG RECORD LENGTH

Syslog records are limited to 1024 bytes. Therefore, the total size of the custom record must not exceed this limit. Custom values and messages that are overridden by the customer must be short and descriptive.

4.3.3. NUMBER OF SYSLOG RECORDS

The product expects one and only one custom Syslog record per transaction.

4.4. Transaction Times

1. The XSLT measures time and latencies of the transaction, one of which is the total latency of the transaction. This value will be slightly less than the real value presented in the latency records, since the response is sent to the client after the XSLT is executed (although the transform action is located after the response action). This means that the latency of transmission to the client will not be included in the measured time of the XSLT. The difference should in most cases be just a few milliseconds.
2. In case the transform action is placed before the result action (**not recommended**), the measured time will have another slight difference compared to the latency records generated by the Gateway. This difference is the latency of the execution of the result action, which follows the transform action. The difference should in most cases be just a few milliseconds.
3. The execution of the XSLT template (without special customizations that might be modified by the customer) has been tested in lab conditions and added a very small overhead of a few milliseconds to the total latency of the transactions.
4. Time analysis of a single transaction that is displayed in the console in transaction level will still be accurate and detailed with the limitation of the existing version, meaning whenever there is a latency syslog record as part of the transaction.

4.5. Request Size in XML Firewall Services

The request size of XML Firewall services cannot be obtained by the XSLT.

4.6. Future Features of the Product

Due to the nature of this solution, it totally depends on the information provided by the XSLT. As the product evolves, it might have in the future features that rely on other sources of information, which cannot be provided by an XSLT. In such a case, those features will not be enabled to customers that rely on the XSLT solution.

5. Customization and deployment

5.1.1. TURN ON CUSTOM TRANSACTION LOG RECORDS

In System Parameters page, set Transactions Source to “logical”.

5.1.2. TESTING CUSTOM TRANSACTION LOG RECORDS

In Transactions page, you should see the custom values that were provided (such as custom service name & IP address).

In Service Activity dashboard, you should see the custom values that were provided (such as custom service name) as well as a new filter - Consumer.

5.1.3. TURN OFF CUSTOM TRANSACTION LOG RECORDS

To turn off this feature and display technical details (the default mode of the product), in System Parameters page, set Transactions Source back to “syslog”.

Insights

This page contains a list of commonly occurring scenarios and how you may resolve them.

- Get request's latency and rate in time series for a service
- Get TPS in time series for a specific domain
- Get TPS in time series for a specific service
- Get TPS in time series for all domains
- Get TPS in time series for all services
- Get TPS in time series for erroneous request for a domain
- Get TPS in time series for erroneous request for a service

TPS = Transaction Per Second (or Request Per second)

Get request's latency and rate in time series for a service

Goto **Dashboards Analytics Service Latency**.

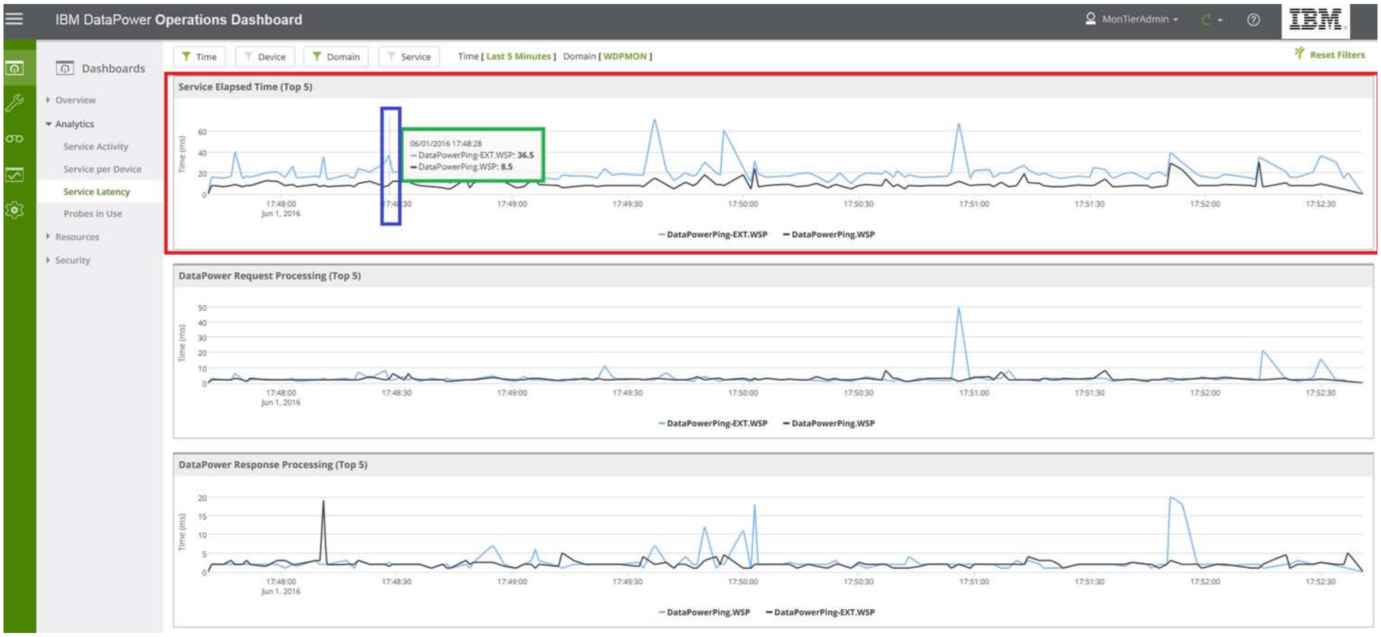
Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

Set **Service Filter** to required service name (Optional).

You will see your time series for each of the TOP5 services in the Legend on the **Service Elapsed Time (Top 5)** - marked in red rectangle.

While point with the mouse on a specific sampling point you can see the rate for this point of time - marked in green rectangle.

You can see below more detailed information on latencies (request, response , backend , inside datapower ...)



Time [Last 5 Minutes] Domain [WDPMON]

06/01/2016 17:48:28
— DataPowerPing-EXT.WSP: 36.5
— DataPowerPing.WSP: 8.5

Get TPS in time series for a specific domain

Goto Dashboards Recent Activity .

Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

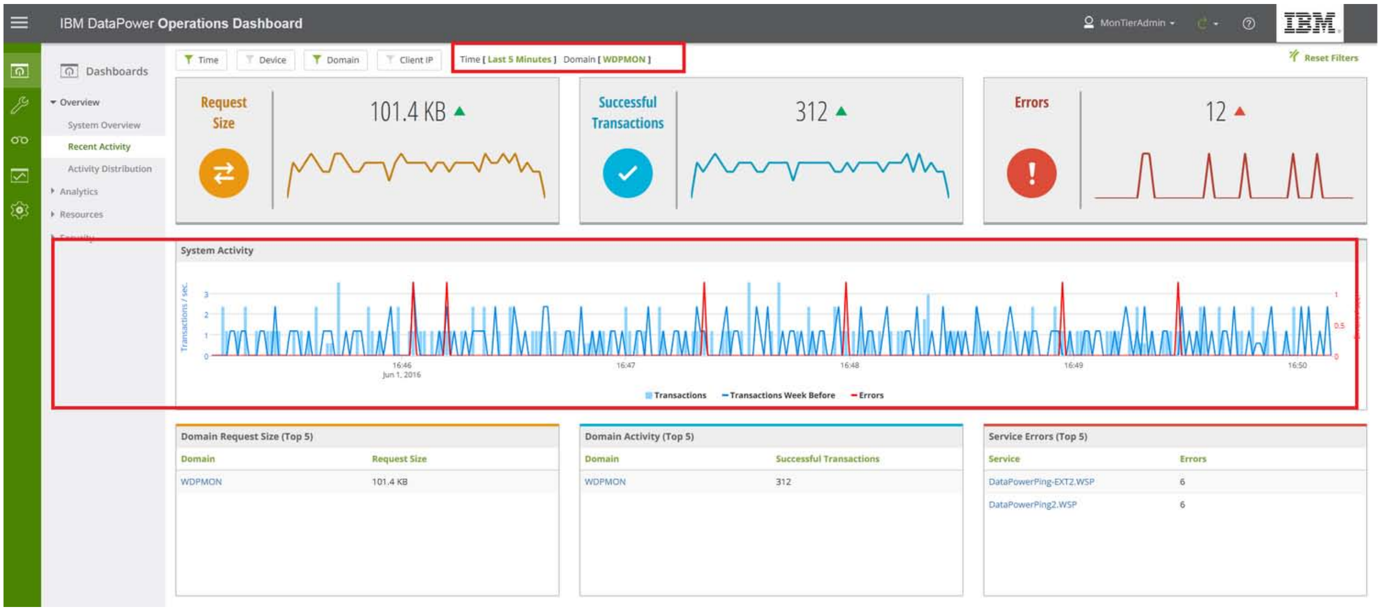
Set **Domain Filter** to the required domain name.

You will see your time series on the System Activity - Marked in Red

The bars shows the current TPS - this is what you look for. please point you mouse on a two close bars and make sure the time diff is 1 second.

The red line show the erroneous service.

the blue line show the transaction TPS week before.



Time [Last 5 Minutes] Domain [WDPMON]

Request Size: 101.4 KB

Successful Transactions: 312

Errors: 12

Domain Request Size (Top 5)

Domain	Request Size
WDPMON	101.4 KB

Domain Activity (Top 5)

Domain	Successful Transactions
WDPMON	312

Service Errors (Top 5)

Service	Errors
DataPowerPing-EXT2.WSP	6
DataPowerPing2.WSP	6

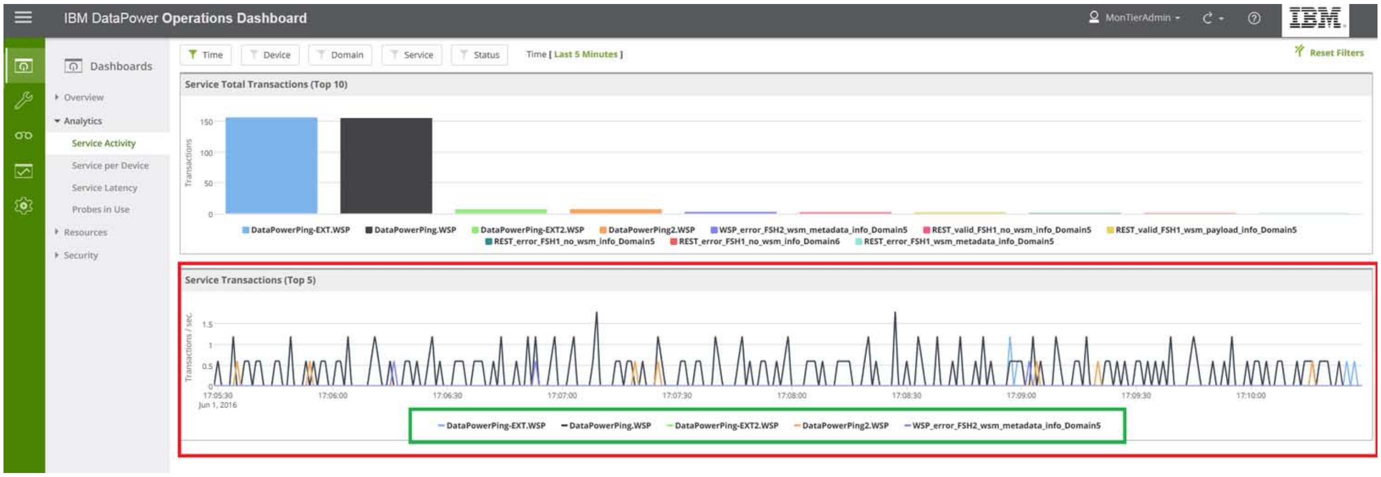
Get TPS in time series for a specific service

Goto Dashboards Analytics Service Activity .

Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

Set **Service Filter** to required service name.

You will see your time series for each of the TOP5 service in the Legend (marked in green) on the **Service Transactions (top 5)** - Marked in Red



Get TPS in time series for all domains

Since you might have a lot o f domains across your IDGs you should choose a set of domains.

We can focus you on the TOP 5 (Or TOP 10) domain activity . Please remember that if you have in 2 IDG's 2 domain with the same name - They will be aggregated unless you filter by device.

Let assume you want to focus on the TOP 5 Domains:

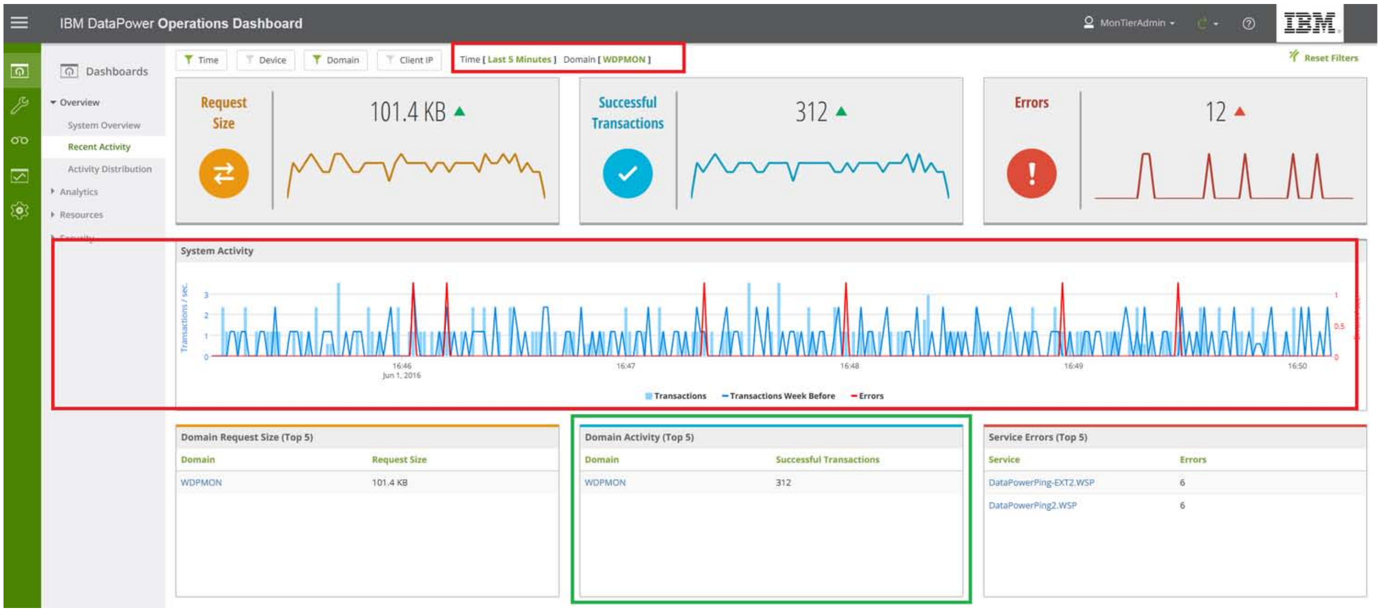
Goto Dashboards Recent Activity .

Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

You will see at the bottom a table labeled with **Domain Activity (Top 5)** - see marked in green

Set **Domain Filter** to each of the domain .

You will see your time series on the System Activity - Marked in Red



Time [Last 5 Minutes] Domain [WDPMON]

Domain Request Size (Top 5)

Domain	Request Size
WDPMON	101.4 KB

Domain Activity (Top 5)

Domain	Successful Transactions
WDPMON	312

Service Errors (Top 5)

Service	Errors
DataPowerPing-EXT2.WSP	6
DataPowerPing2.WSP	6

Get TPS in time series for all services

Since you might have a lot of services across your IDGs you should choose a set of services .

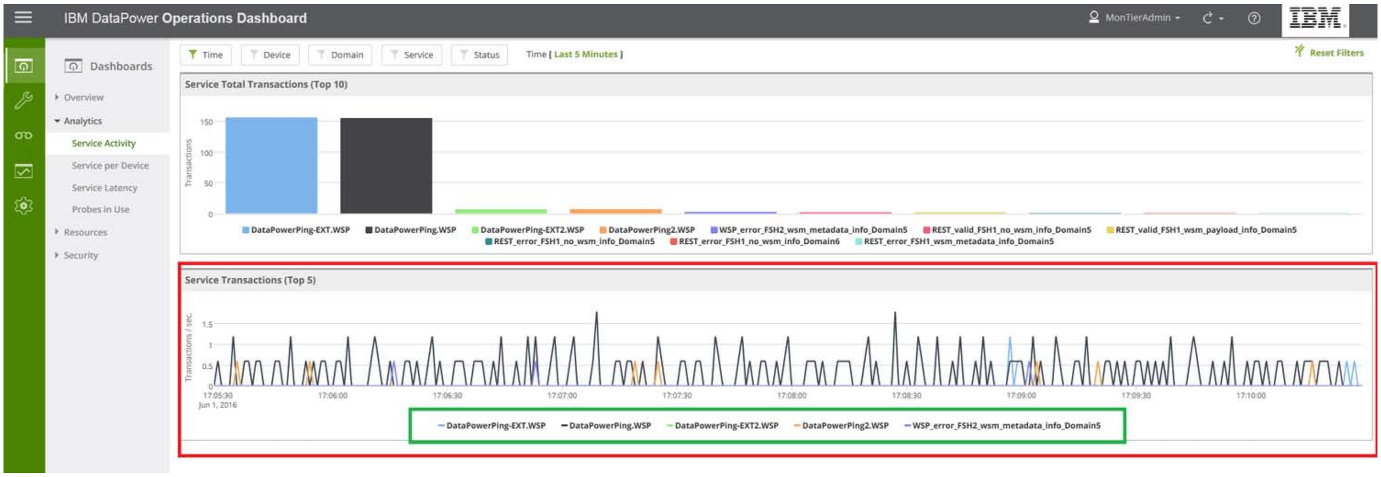
We can focus you on the TOP 5 (Or TOP 10) domain activity . Please remember that if you have in 2 IDG's 2 domain with the same name - They will be aggregated unless you filter by device.

Let assume you want to focus on the TOP 5 Services:

Goto Dashboards Analytics Service Activity .

Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

You will see your time series for each of your TOP 5 domain (Mark in Green) on the same graph on the **Service Transaction (Top 5)** - Marked in Red



Get TPS in time series for erroneous request for a domain

Actually We show the overall transaction rate, the erroneous transaction rate and the last week transaction rate on the same graph.

Please visit for detailed explanation Get TPS in time series for a specific domain

Get TPS in time series for erroneous request for a service

Goto Dashboards Analytics Service Activity .

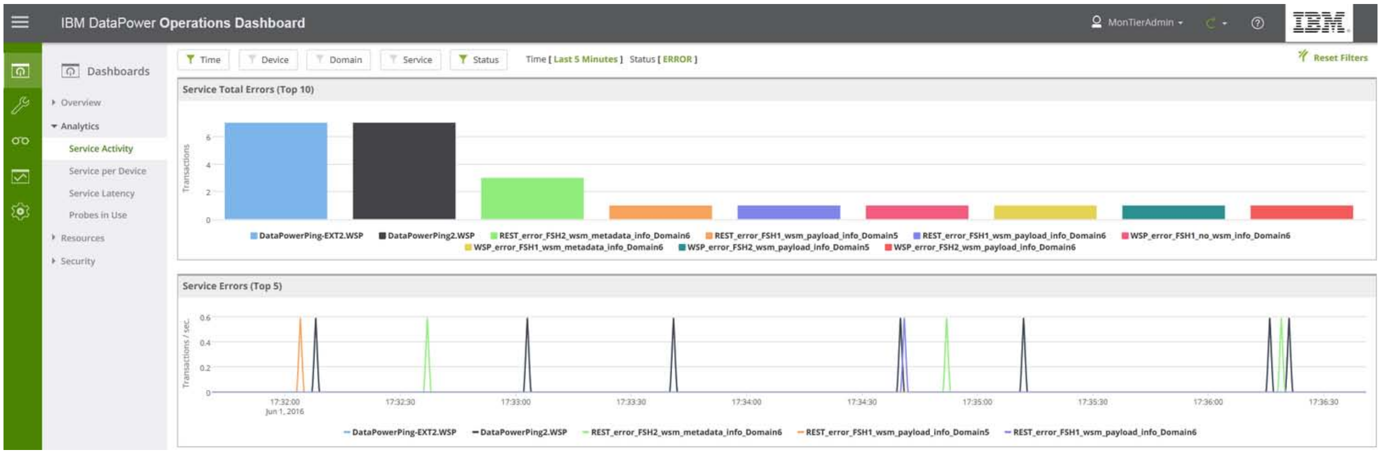
Set **Time Filter** to 5 minutes (this is usually generates a 1 sec interval).

Set **Service Filter** to required service name (Optional).

Set **Status Filter** to ERROR.

You will see your time series for each of the TOP5 service in the Legend (marked in green) on the **Service Transactions (top 5)**

On the **Service Total Errors (Top 10)** you can see the total count (for the period of the filter).



Time [Last 5 Minutes] Status [ERROR]

IBM DataPower Operations Dashboard
MonTierAdmin
Dashboards
Overview
Analytics
Service Activity
Service per Device
Service Latency
Probes in Use
Resources
Security
Time
Device
Domain
Service
Status
Reset Filters
Service Total Errors (Top 10)
Transactions
6
4
2
0
DataPowerPing-EXT2.WSP
DataPowerPing2.WSP
REST_error_FSH2_wsm_metadata_info_Domain6
REST_error_FSH1_wsm_payload_info_Domain5
REST_error_FSH1_wsm_payload_info_Domain6
WSP_error_FSH1_no_wsm_info_Domain6
WSP_error_FSH1_wsm_metadata_info_Domain6
WSP_error_FSH2_wsm_payload_info_Domain5
WSP_error_FSH2_wsm_payload_info_Domain6
Service Errors (Top 5)
Transactions / sec.
0.6
0.4
0.2
0
17:32:00
Jun 1, 2016
17:32:30
17:33:00
17:33:30
17:34:00
17:34:30
17:35:00
17:35:30
17:36:00
17:36:30
DataPowerPing-EXT2.WSP
DataPowerPing2.WSP
REST_error_FSH2_wsm_metadata_info_Domain6
REST_error_FSH1_wsm_payload_info_Domain5
REST_error_FSH1_wsm_payload_info_Domain6