

Course Guide

Administration of IBM DataPower Gateway V7.6

Course code WE761 / ZE761 ERC 1.0



February 2018 edition

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on 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, MD-NC119
Armonk, NY 10504-1785
United States of America*

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 jurisdictions 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 and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

© Copyright International Business Machines Corporation 2018.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Trademarks	x
Course description	xi
Agenda	xiii
Unit 1. DataPower deployment environments	1-1
Unit objectives	1-2
DataPower deployment environments	1-3
IBM DataPower Gateway: Rack mounting	1-4
Physical IBM DataPower Gateway: Front view	1-5
Physical IBM DataPower Gateway: Rear view	1-8
Connecting to the DataPower gateway serial connector	1-10
Connecting the physical gateway to the network	1-11
More on the virtual gateway	1-12
IBM DataPower Gateway Virtual Editions	1-13
Virtual gateways for VMware hypervisors	1-14
Deployment on VMware hypervisors	1-15
Virtual gateways for Citrix XenServer hypervisor	1-16
Deployment on Citrix XenServer hypervisors	1-17
Virtual gateways for Linux	1-18
Deployment on Linux	1-19
Network interfaces for virtual gateways	1-20
Migrating a virtual XI or XG to a virtual IDG	1-21
DataPower in the cloud	1-22
Downloading DataPower Gateway for Developers on Docker	1-23
DataPower Software Product Compatibility Reports: 1 of 2	1-24
DataPower Software Product Compatibility Reports: 2 of 2	1-25
Differences in capabilities in the deployment options	1-26
Unit summary	1-27
Review questions	1-28
Review answers	1-29
Unit 2. Initial setup	2-1
Unit objectives	2-2
Starting a gateway	2-3
Starting a DataPower physical gateway	2-4
Starting a DataPower virtual gateway	2-5
Initializing or reinitializing the gateway (1 of 2)	2-6
Initializing or reinitializing the gateway (2 of 2)	2-7
Administration by using the command-line interface	2-8
Initial CLI login screen	2-9
Quick initial configuration procedure	2-10
Accept the license agreement by using the WebGUI	2-11
Access the WebGUI	2-12
Access to the Blueprint Console	2-13
Web management graphical interface certificate error	2-14
Generate a gateway certificate	2-15
Typical interface topology	2-16
Defining Ethernet interfaces in the WebGUI	2-17

Defining a specific Ethernet interface: Main tab	2-18
DNS settings	2-19
Time and date settings	2-20
Configure management services	2-21
Set basic RBM settings: Password policy tab	2-22
Set basic RBM settings: Account policy tab	2-23
Configure system settings	2-24
Create a secondary administrative account	2-25
Custom user interface file	2-26
Custom user interface file: WebGUI example	2-27
Custom user interface file: CLI example	2-29
Auxiliary storage	2-30
Preparing the RAID array (1 of 3)	2-31
Preparing the RAID array (2 of 3)	2-32
Preparing the RAID array (3 of 3)	2-33
Auxiliary storage on the virtual gateway	2-34
Globalization: Displaying other languages in the Web Management service and the log	2-35
Enabling languages	2-36
Getting the WebGUI to display an alternative language	2-37
Getting an alternative language for the log and messages	2-38
Unit summary	2-39
Review questions	2-40
Review answers	2-41
Unit 3. Managing firmware.....	3-1
Unit objectives	3-2
Actions on firmware	3-3
Release names	3-4
Restrictions for the actions on firmware	3-5
Requirements to perform an upgrade	3-6
Suggested procedure for upgrading	3-7
Step 1. Identify features with feature-specific libraries	3-8
Step 2. Determine the firmware image to download	3-9
Step 3. Download the firmware image from Fix Central	3-10
Step 4. Back up the current gateway configuration	3-11
Step 5. Optional: Restart the gateway	3-12
Step 6. Transfer the downloaded firmware image	3-13
Step 7. Install the firmware image	3-14
Step 8. Verify the upgrade operation	3-15
Roll back the firmware	3-16
Add-on module and feature management	3-17
Product packaging: optional modules	3-18
Product packaging: physical gateway optional modules	3-20
Product packaging: virtual gateway optional modules	3-21
Tenant feature (1 of 5)	3-22
Tenant feature (2 of 5)	3-23
Tenant feature (3 of 5)	3-24
Tenant feature (4 of 5)	3-25
Tenant feature (5 of 5)	3-26
Unit summary	3-27
Review questions	3-28
Review answers	3-29
Exercise 1	3-30
Exercise objectives	3-31

Unit 4. DataPower administration overview	4-1
Unit objectives	4-2
DataPower Appliance administration	4-3
Web management interface	4-4
Web management login page	4-5
Main page for Blueprint Console	4-6
Main page for WebGUI	4-7
Switching between Blueprint Console and WebGUI	4-8
Navigation bar categories	4-9
System control features (1 of 3)	4-10
System control features (2 of 3)	4-11
System control features (3 of 3)	4-13
File management	4-15
File directories for configuration	4-16
File directories for security	4-17
File directories for logging	4-18
More file directories	4-19
Administrative access control	4-20
Create application domains, user groups, and users	4-21
Saving configuration changes	4-22
Controlling the resource limits of the gateway	4-23
Notifying on gateway failure	4-24
Administration by using the command-line interface	4-25
Administration by using the XML Management Interface	4-26
Administration by using the REST Management Interface	4-27
Management interface summary	4-28
Appliance and services status	4-29
Secure backup mode	4-30
Determining current Backup mode	4-31
Perform a secure backup	4-32
Restoring a gateway (1 of 3)	4-33
Restoring a gateway (2 of 3)	4-35
Restoring a gateway (3 of 3)	4-36
Quiescence	4-37
Unit summary	4-38
Review questions	4-39
Review answers	4-40
Unit 5. Using CLI and the XML Management Interface to configure appliance	5-1
Unit objectives	5-2
Administrative interfaces	5-3
Enable the SSH CLI interface	5-4
CLI users	5-5
RBM settings and CLI	5-6
Controlling access in a User Account object	5-7
Controlling access in a User Group object	5-8
Global configuration mode	5-9
Entering and leaving a configuration mode (1 of 2)	5-10
Entering and leaving a configuration mode (2 of 2)	5-11
Create and update objects over CLI	5-12
Common commands	5-13
Retrieve system information by using CLI	5-14
Ethernet interfaces (1 of 2)	5-15
Ethernet interfaces (2 of 2)	5-17
Associate Ethernet interface to administrative service	5-18
Network utilities	5-19

Monitoring commands	5-20
Troubleshooting commands	5-21
Scripting commands	5-22
Alias command	5-23
Copying files	5-24
The exec command	5-25
User and domain configuration: Step 1: Create a domain	5-26
User and domain configuration: Step 2: Create a user group	5-27
User and domain configuration: Step 3: Create a user	5-28
Configuration files	5-29
CLI commands in the information center	5-30
Administration by using the XML Management Interface (XMI)	5-31
WebGUI setup of the XML Management Interface	5-32
Administration by using SOAP	5-33
Communicating with the XML Management Interface	5-34
SOAP Configuration Management (SOMA)	5-35
Sample SOMA request	5-36
Using cURL to issue the status request	5-37
SOMA: Get status information	5-38
SOMA: Status information response (1 of 2)	5-39
SOMA: Status information response (2 of 2)	5-40
Perform actions: Perform administrative actions	5-41
SOMA: Create a configuration object	5-42
SOMA: Domain creation response	5-43
SOMA: Delete configuration objects	5-44
SOMA: Modify configuration objects	5-45
Error handling	5-46
Appliance Management Protocol (AMP)	5-47
AMP request: Get domain list	5-48
AMP request: Get domain list request message	5-49
AMP request: Get domain list response	5-50
REST Management Interface	5-51
REST Management Interface	5-52
The REST high-level resources	5-53
Sample REST requests: status request	5-55
Sample REST requests: get User configuration	5-56
Sample REST requests: create a User	5-57
Administration by using the web management interface	5-58
The web interface navigation bar	5-59
Unit summary	5-60
Review questions	5-61
Review answers	5-62
Exercise 2	5-63
Exercise objectives	5-64
Exercise overview (1 of 3)	5-65
Exercise overview (2 of 3)	5-66
Exercise overview (3 of 3)	5-67
Unit 6. DataPower services overview	6-1
Unit objectives	6-2
Services in a DataPower gateway	6-3
Front sides and back sides, and sideways	6-4
Services available on the DataPower gateway	6-5
XML firewall service	6-6
Multi-protocol gateway service	6-7
Web service proxy service	6-8

B2B gateway service	6-9
Access manager reverse proxy	6-10
Web application firewall service	6-11
Other services	6-12
Which service type should you use?	6-13
Unit summary	6-14
Review questions	6-15
Review answers (1 of 2)	6-16
Review answers (2 of 2)	6-17
Unit 7. Using the Web Management Blueprint Console to configure appliance	7-1
Unit objectives	7-2
Getting to the Blueprint Console	7-3
Administrative access control	7-4
Separate or grouped application domains	7-5
Create an application domain	7-6
Configuration mode of an application	7-7
View application domain status	7-8
Configuration Checkpoints	7-9
Manage user group details	7-10
Example: Access profile for the student admin group	7-11
Manage a user account	7-12
Role-base management (RBM)	7-13
RBM policy processing	7-14
Using RBM for the Web Management service	7-15
Configure RBM authentication for WebGUI	7-16
RBM authentication methods	7-17
Configure LDAP RBM authentication method	7-18
RBM authorization for the Web Management service	7-19
XML file: RBM policy file for authorization	7-20
Unit summary	7-21
Review questions	7-22
Review answers	7-23
Unit 8. Troubleshooting	8-1
Unit objectives	8-2
Common problem determination tools	8-3
Gateway status information	8-4
Troubleshooting	8-5
How to get to the Troubleshooting page	8-6
Troubleshooting: Networking	8-7
Troubleshooting: Packet capture	8-8
Troubleshooting: Logging	8-9
Troubleshooting: System log	8-10
Filtering system log	8-11
Troubleshooting: Generate Log Event	8-12
Troubleshooting: Reporting	8-13
Troubleshooting: Advanced	8-14
Troubleshooting: XML File Capture	8-15
Troubleshooting: Send a test message	8-16
Troubleshooting: Multi-step probe	8-17
Troubleshooting: Enabling the multi-step probe	8-18
Multi-step probe transaction list	8-19
Multi-step probe content	8-20
Debugging GatewayScript (1 of 4)	8-21
Debugging GatewayScript (2 of 4)	8-22

Debugging GatewayScript (3 of 4)	8-24
Debugging GatewayScript (4 of 4)	8-25
Problem determination with cURL	8-26
Communicating with DataPower support	8-27
Unit summary	8-28
Review questions	8-29
Review answers	8-30
Exercise 3	8-31
Exercise objectives	8-32
MyBasicMPG.zip	8-33
Unit 9. DataPower cryptographic tools and SSL setup	9-1
Unit objectives	9-2
DataPower use of keys and certificates	9-3
Creating a private key and certificate	9-4
Generating crypto (asymmetric) keys onboard (1 of 2)	9-5
Generating crypto (asymmetric) keys onboard (2 of 2)	9-6
Download keys from temporary storage	9-7
Key and certificate objects point to files	9-8
Crypto shared secret (symmetric) key	9-9
Crypto (asymmetric) key	9-10
Crypto certificate	9-11
Crypto identification credential	9-12
Example: Display details of a crypto file	9-13
Crypto validation credential	9-14
Import and export crypto objects	9-15
Certificates can expire or get revoked	9-16
Certificate revocation list (CRL) retrieval	9-17
Crypto certificate monitor	9-18
Hardware Security Module (HSM)	9-19
Remote Hardware Security Module (HSM)	9-20
DataPower support for SSL	9-21
SSL profiles	9-22
SSL - crypto object relationships	9-23
DataPower as the SSL server (from client to gateway) (1 of 2)	9-24
DataPower as the SSL server (from client to gateway) (2 of 2)	9-25
DataPower as the SSL client (from gateway to back-end server) (1 of 2)	9-26
DataPower as the SSL client (from gateway to back-end server) (2 of 2)	9-27
Securing connection from gateway to external resource server	9-28
What is a “user agent”?	9-29
Configuring a user agent (1 of 2)	9-30
Create a user agent configuration (2 of 2)	9-31
SSL SNI server profile (1 of 2)	9-32
SSL SNI server profile (2 of 2)	9-33
SSL Host Name Mapping	9-34
The SSL proxy profile (deprecated)	9-35
A crypto profile (deprecated) specifies details of the SSL connection	9-36
Crypto profile (deprecated)	9-37
Proxy profile - crypto object relationships (deprecated)	9-38
Unit summary	9-39
Review questions (1 of 2)	9-40
Review questions (2 of 2)	9-41
Review answers (1 of 2)	9-42
Review answers (2 of 2)	9-43
Exercise 4	9-44
Exercise objectives	9-45

Exercise overview (1 of 2)	9-46
Exercise overview (2 of 2)	9-47
Unit 10. Logging and log targets.....	10-1
Unit objectives	10-2
Logging on the DataPower Gateway	10-3
Logging basics	10-4
Available log levels	10-5
Event categories	10-6
Event codes (1 of 2)	10-7
Event codes (2 of 2)	10-8
Log targets	10-9
Manage Log targets: Main	10-10
Log target types	10-12
Manage Log targets: Event filters	10-13
Manage Log targets: Object filters	10-14
Manage Log targets: IP address filters	10-15
Manage Log targets: Event trigger	10-16
Manage Log targets: Event subscriptions	10-17
Example: Create a log category	10-18
Example: Display the log category	10-19
Example: Generate a Log event	10-20
Example: View the event in the system log	10-21
Application-specific logging: Audit log	10-22
Unit summary	10-23
Review questions	10-24
Review answers	10-25
Exercise 5	10-26
Exercise objectives	10-27
Unit 11. Course summary	11-1
Unit objectives	11-2
Course objectives	11-3
Lab exercise solutions	11-4
To learn more on the subject	11-5
Unit summary	11-6
Appendix A. List of abbreviations	A-1

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

Approach®

DB™

Express®

Notes®

Tivoli®

Bluemix®

DB2 Connect™

IBM Business Partner®

Power®

WebSphere®

DataPower®

DB2®

IMS™

Rational®

z/OS®

Intel and Intel Core are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Lenovo and ThinkPad are trademarks or registered trademarks of Lenovo in the United States, other countries, or both.

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

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

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

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

VMware is a registered trademark or trademark of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

CloudLayer® and SoftLayer® are trademarks or registered trademarks of SoftLayer, Inc., an IBM Company.

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

Course description

Administration of IBM DataPower Gateway V7.6

Duration: 2.5 days

Purpose

IBM DataPower Gateway Appliances are network devices that help secure, integrate, and optimize access to web, web services, mobile, and API workloads. Through instructor-led lectures and hands-on lab exercises, you learn how to run various administrative procedures, from initial installation and setup through ongoing maintenance of the appliances in production. You learn about the available management interfaces, such as the command-line interface (CLI), Web Management graphical interface, and XML Management Interface. You also learn how to use these interfaces to run various administrative tasks, such as upgrading firmware, running backup and restore operations, and configuring user accounts and domains.

This course exercises uses the following appliances:

- DataPower Gateway Virtual Edition

Information in the course units also applies to other DataPower appliances.

The course includes some information on upgrading firmware and working with DataPower hardware appliances.

The lab environment for this course uses the Ubuntu Linux Operating System on an ESX image that runs on the IBM Remote Lab Platform.

Audience

This course is designed for administrators who install, manage, and monitor IBM DataPower Gateway Appliances. The course is also relevant for developers who administer appliances.

Prerequisites

Before taking this course, you should successfully complete course VW700, *Technical Introduction to IBM WebSphere DataPower Gateway Appliances V7*. You should also be familiar with:

- Security-based concepts and protocols
- Ubuntu Linux
- Networking protocols

Objectives

- Configure an appliance for its initial deployment
- Download and upgrade the firmware on the DataPower appliances

- Create and manage user accounts, groups, and domains
- Configure Secure Sockets Layer (SSL) to and from DataPower Appliances
- Troubleshoot and debug services by using the problem determination tools, logs, and probes that are provided with the DataPower appliance
- Configure logging of messages to external locations

Agenda

**Note**

The following unit and exercise durations are estimates, and might not reflect every class experience.

Day 1

- (00:15) Course introduction
- (00:30) Unit 1. DataPower deployment environments
- (01:15) Unit 2. Initial setup
- (00:30) Unit 3. Managing firmware
- (00:30) Exercise 1. Upgrading image firmware
- (01:15) Unit 4. DataPower administration overview
- (01:30) Unit 5. Using CLI and the XML Management Interface to configure appliance access

Day 2

- (01:30) Exercise 2. Using the CLI and the XML Management Interface to manage DataPower appliances
- (00:30) Unit 6. DataPower services overview
- (00:30) Unit 7. Using the Web Management Blueprint Console to configure appliance access
- (00:45) Unit 8. Troubleshooting
- (01:00) Exercise 3. Using the troubleshooting tools to debug errors
- (01:00) Unit 9. DataPower cryptographic tools and SSL setup

Day 3

- (01:00) Exercise 4. Securing connections with SSL
- (00:30) Unit 10. Logging and log targets
- (01:00) Exercise 5. Logging to an external system
- (00:15) Unit 11. Course summary

Unit 1. DataPower deployment environments

Estimated time

00:30

Overview

This unit presents the various environments that a DataPower gateway can be deployed into. A DataPower gateway can still be deployed as a physical appliance, although there are many options for deployment of a virtual edition of the gateway. The VMware, Citrix, Linux, Docker, and cloud possibilities are listed. The Software Product Compatibility Report is reviewed, which lists the specific operating environments for DataPower, and the other products and versions that DataPower interacts with.

How you will check your progress

- Review questions

References

IBM DataPower Gateways Version 7.6.0 product documentation:

http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0

Unit objectives

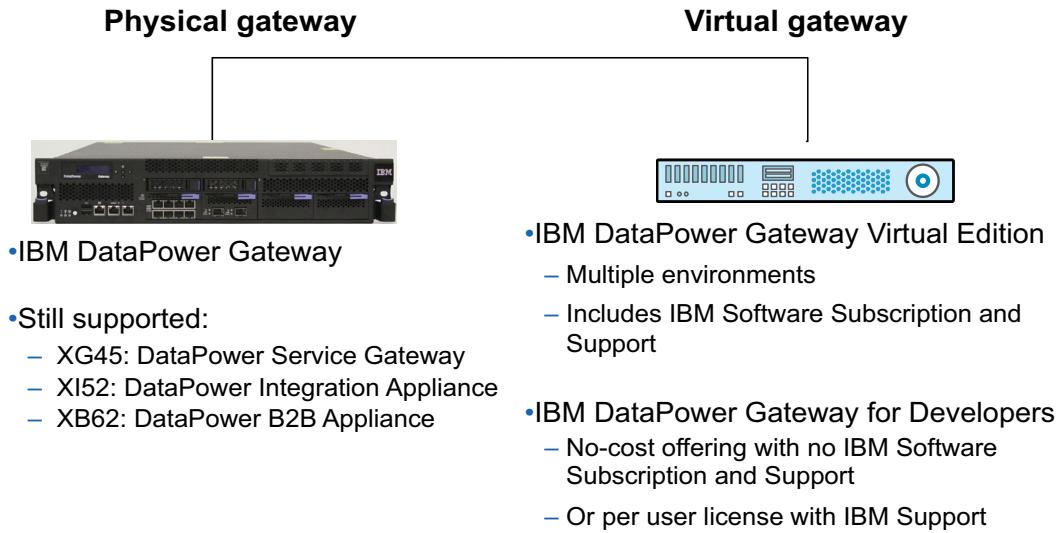
- Identify the different editions of the Virtual Edition, and how they differ
- Describe the DataPower deployment options
- List some of the physical characteristics of the DataPower hardware
- Describe the Ethernet interface options for the physical and virtual gateway
- List the supported runtime environments for the Virtual Edition
- List the basic steps for deploying a virtual gateway in the VMware, Citrix, Linux, and Docker environments
- List the supported cloud environments for the virtual gateway
- Describe the Docker support for DataPower
- Describe how to request and use a Software Product Compatibility Report

Figure 1-1. Unit objectives

DataPower deployment environments

The DataPower capabilities are delivered in multiple deployment options to meet your needs

Physical, virtual, cloud, Linux, or Docker



[DataPower deployment environments](#)

© Copyright IBM Corporation 2018

Figure 1-2. DataPower deployment environments

IBM DataPower Gateway is available in physical, virtual, cloud, Linux, and Docker form factors.

IBM DataPower Gateway: Rack mounting

- This physical gateway is rack-mounted:
 - 2U form factor
 - Requires both a front and a rear mounting support
 - Front side contains Ethernet ports
 - Rear side contains a power supply, battery tray, and auxiliary storage
 - Older XG45 is a 1U form factor, XI52 and XB62 are a 2U form factor
- Connectivity
 - Two power cords
 - Ethernet cables (RJ45 and SFP+)
 - Serial port (RJ45 connector)



DataPower deployment environments

© Copyright IBM Corporation 2018

Figure 1-3. IBM DataPower Gateway: Rack mounting

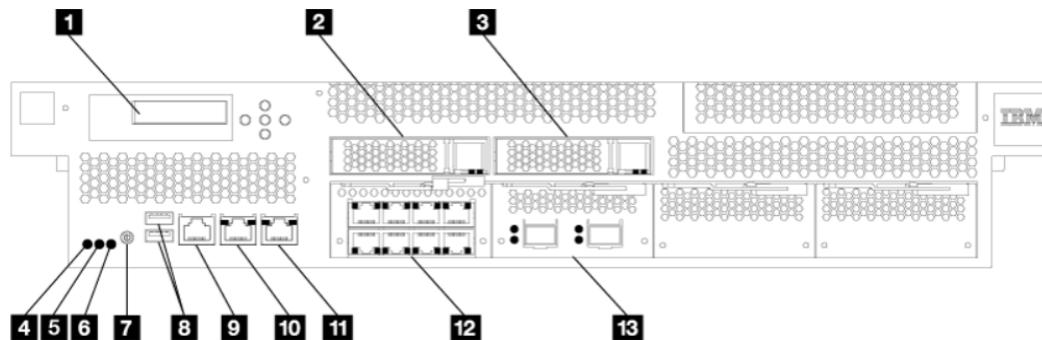
A rack unit (abbreviated as U or RU) is a unit of measurement defined as 1.75 inches (44.5 millimeters).

For more information and the detailed step-by-step instructions on how to install the gateway into a rack, see the product documentation installation guide.

The picture is of two XI52s in a rack in an IBM data center. The IBM DataPower Gateway is very similar. The yellow cable connects the console connector to a remote serial server. The light blue cable connects MGT0 to the network. The dark blue cable connects ETH10 to the network. The black cable connects ETH11 to the network.

Physical IBM DataPower Gateway: Front view

- The front of the DataPower gateway contains:
 - 12 Ethernet connections (10, 11, 12,13): 10 RJ45, 2 SFP+
 - One console connector (9)
 - Two hard disk drive modules (2, 3)
 - Numerous LED indicators



DataPower deployment environments

© Copyright IBM Corporation 2018

Figure 1-4. Physical IBM DataPower Gateway: Front view

The image shows the following parts of the front view (type 8436):

- LCD display
- Hard disk drive 1
- Hard disk drive 2
- Fault LED
- Locate LED
- Power LED
- Power button
- Two USB ports
- Console connector
- mgt0 management port
- mgt1 management port
- 1 Gb Ethernet module
- 10 Gb Ethernet module

- **LCD module**

The front panel has a liquid crystal display (LCD) module that includes an LCD and five menu choices. The LCD provides information about the model type of the gateway; however, the menu choices are not functional.

- **Hard disk drive modules**

The front panel includes 2.5-inch hard disk drive modules.

- **Fault LED**

The amber fault LED is illuminated when the gateway detects a critical hardware event.

- **Locate LED**

The blue locate LED is illuminated when the DataPower firmware activates it. You can control whether this LED is illuminated from the web management interface or from the command line. The LED remains lit until deactivated.

- **Power LED**

The power LED is illuminated when the gateway is connected to a power source and you turn on the gateway.

The green power LED is illuminated when the gateway is on and fully functioning.

If the LED is not illuminated, the gateway is turned off.

- **Power button**

The power button is on the front panel of the gateway. Press the power switch to:

- Turn on the gateway.
- Shut down the gateway properly (if the gateway is already turned on).

- **USB ports**

The front panel has a USB interface that conforms to USB 2.0 devices. This USB connectors are not enabled and do not provide any connection.

- **Console connector**

The front panel has a console connector. The console connector is an eight-position modular jack (ISO 8877, often called RJ45). For initial configuration, use the supplied cable to connect from an ASCII terminal1 to the gateway or to connect from a PC that is running terminal emulation software to the gateway.

- **Network connectors**

The front panel has two LAN management Ethernet ports and two Ethernet modules.

- **LAN management Ethernet ports**

The MGT0 and MGT1 management Ethernet ports provide connection to the LAN. These ports provide remote management access to the gateway and should not be used as data ports. Use the interfaces in the Ethernet modules for handling data traffic and for logging functions to and from the DataPower services.

Approach: Use the MGT0 or MGT1 Ethernet interface for system-wide management functions to handle network traffic for incoming SNMP, SSH, and web management functions on your intranet.

- MGT0 Ethernet connector

This Ethernet interface can manage all transaction data on the gateway. The MGT0 Ethernet connector also supports IPMI over LAN, including serial over LAN.

- MGT1 Ethernet connector

This Ethernet interface can manage all transaction data on the gateway.

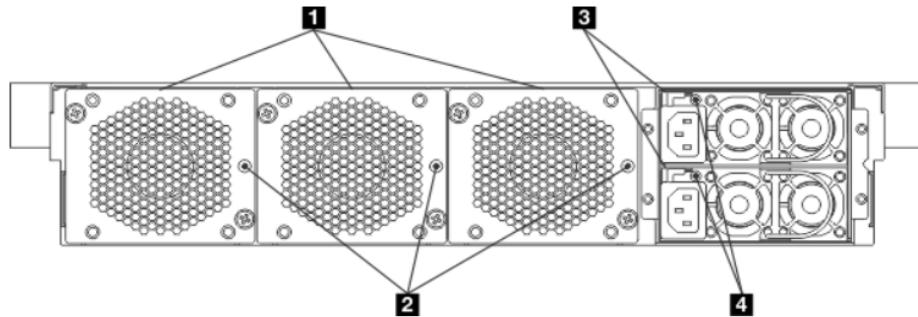
- **Ethernet modules**

The DataPower gateway has two Ethernet modules for Ethernet connectivity. Use the interfaces in the Ethernet modules for handling data traffic and for logging functions to and from the DataPower services.

- The 1Gb Ethernet module contains 8 ports and associated LEDs. The ports are labeled as ETH10-ETH17
- The 10Gb Ethernet module contains 2 small-form-factor pluggable (SFP+) ports and associated LEDs. The ports are labeled as ETH20-ETH21. SFP+ ports support optical or electrical interfaces with the appropriate transceiver.

Physical IBM DataPower Gateway: Rear view

- The rear of the DataPower gateway contains:
 - Two power supplies (3)
 - Three fan trays (1)
 - LED indicators for each power supply (4) and fan (2)



- The customer can replace the power supplies, fans, battery, and auxiliary storage units

Figure 1-5. Physical IBM DataPower Gateway: Rear view

The image shows the following parts of the rear view (type 8436):

1. Fan modules
2. Fan LEDs
3. Power supply modules
4. Power supply module LEDs

- Fan modules**

The gateway has three fan modules. Each fan module contains cooling fans with an LED that indicates the status of the module.

- Amber single flash shows when power is first applied to the fan module.
- Amber steady light indicates that the fan is operating at less than 1200 RPM or there is a fault in the module.
- No illumination when there is no power present or there is no problem.

The speed of the fans depends on the temperature of the gateway. As the temperature increases, the fan speed increases to maintain a balanced temperature.

- **Power supply modules**

The gateway has two redundant power supply modules. A single power supply module can supply the power to support gateway operations. You can hot-swap the power supply modules. In other words, you can replace a power supply module without powering down the gateway. Each power supply module contains an LED that indicates the status of the module.

- If the LED is illuminated in green, the gateway is connected to a power source and fully functioning.
- If the LED is red, the module is not functioning within design specifications.
- If the LED is not illuminated, there is no power to the module.

Connecting to the DataPower gateway serial connector

Initial setup requires a connection to the console connector of the DataPower gateway

- Use the cable that is included with the DataPower gateway to connect from the front panel to either:
 - ASCII terminal
 - PC running terminal emulation software (for example, PuTTY)



DataPower deployment environments

© Copyright IBM Corporation 2018

Figure 1-6. Connecting to the DataPower gateway serial connector

The console connector on the front panel is a RJ45 connector. Two cables are supplied with the gateway: a RJ45-to-DB9 cable, and a RJ45-to-USB cable.

Ensure that the terminal or PC is configured for standard 9600 8N1 and no flow control operation. 8N1 is a notation for a serial configuration in asynchronous mode, where there are 8 data bits, no (N) parity bit, and 1 stop bit.

Always maintain a serial port connection to the gateway in the event of a network failure. It provides a backup mechanism for network administrators to access the gateway. The drawback of the serial cable is that it requires someone to physically connect the cable to the gateway. Although this drawback is true during the initial setup, you can set up the gateway to a console server to enable remote access to the gateway when using the serial port.

The PuTTY website is at: <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Connecting the physical gateway to the network

- Connect the Ethernet ports of the DataPower gateway to neighboring network devices, such as a switch or load balancer
- The following modes are available for the Ethernet interfaces:
 - **Auto:** Uses auto-negotiation
 - **10baseT-FD:** Forces 10BASE-T PHY (10 Mbps) in full-duplex mode
 - **10baseT-HD:** Forces 10BASE-T PHY (10 Mbps) in half-duplex mode
 - **100baseTx-FD:** Forces 100BASE-TX PHY (100 Mbps) in full-duplex mode
 - **100baseTx-HD:** Forces 100BASE-TX PHY (100 Mbps) in half-duplex mode
 - **1000baseTx-FD:** Uses 1000BASE-T PHY, which is always full-duplex
- On physical appliances, you cannot modify the operational mode for Ethernet interfaces that use 10-gigabit ports.



- Ethernet speeds on virtual appliances are controlled by the host

DataPower deployment environments

© Copyright IBM Corporation 2018

Figure 1-7. Connecting the physical gateway to the network

More on the virtual gateway

- The Virtual Edition comes in three “editions” for differing deployments:
 - DataPower Gateway Virtual Edition
 - For production environments
 - Charged by the Processor Value Unit (PVU)
 - DataPower Gateway Virtual Edition for Nonproduction environments
 - For development and testing
 - Charged by the Processor Value Unit (PVU)
 - DataPower Gateway Virtual Edition for Developers
 - For development and testing
 - Charged by the user
- Virtual Edition is ordered from Passport Advantage (PPA)

Figure 1-8. More on the virtual gateway

The DataPower Gateway Virtual Editions for Production and Nonproduction can be deployed to a Linux operating system or a Linux-based hypervisor.

The DataPower Gateway Virtual Edition for Developers can run as a guest in the VMware products that support virtual hardware version 10 or higher.

These deployments are covered later in this presentation unit.

IBM DataPower Gateway Virtual Editions

- Downloaded from IBM Passport Advantage (PPA)

Supported environments:

- Production and Nonproduction editions
 - RHEL Client/Server/Workstation 7
 - Ubuntu 14.04/16.04 LTS
 - VMware ESXi 5.5/6.0/6.5
 - Citrix XenServer 6.2/6.5
 - IBM PureApplication System W1500/W2500 Version 2.0
 - SoftLayer bare metal dedicated servers/CCI
 - Amazon EC2/Microsoft Azure virtual server
- Developers edition
 - VMware Fusion Version 8
 - VMware Workstation Pro Version 12
- See the DataPower Gateway V7.6.0 announcement letter, the Knowledge Center, and the Software Product Compatibility Report for more details on supported environments and hardware requirements

DataPower deployment environments

© Copyright IBM Corporation 2018

Figure 1-9. IBM DataPower Gateway Virtual Editions

“RHEL” is Red Hat Enterprise License.

“CCI” refers to SoftLayer CloudLayer Computing Instance

The V7.6.0 announcement letter is at

http://www.ibm.com/common/ssi>ShowDoc.wss?docURL=/common/ssi/rep_ca/5/897/ENUS217-265/index.html&request_locale=en#hardx

The Software Product Compatibility Report is discussed later in this unit.

Virtual gateways for VMware hypervisors

- Delivered as an .ova file (open virtual gateway/application)
 - XML descriptor file
 - 16 GB encrypted virtual disk that contains the firmware and configuration data
 - 16 GB virtual disk to contain the RAID volume data
- Naming convention:
 - xxx.prod.ova (Production edition)
 - xxx.nonprod.ova (Nonproduction edition)
 - xxx.dev.ova (Developers edition)
- During deployment, disk allocation depends on the provisioning option:
 - Thin provisioning: 258.6 MB, expand as needed
 - Thick: 32 GB
- Minimum resource allocation:
 - Without API workload, 4 vCPU and 4 GB RAM
 - Developers edition: 2 vCPU and 4 GB RAM
 - With API workload, 4 vCPU and 8 GB RAM

[DataPower deployment environments](#)

© Copyright IBM Corporation 2018

Figure 1-10. Virtual gateways for VMware hypervisors

The prefix for the OVA file name varies with the specific firmware version.

“vCPU” is “virtual CPU”.

The Production edition has named resource configurations:

- “Small” is 4 vCPU and 8 GB RAM
- “Standard” is 8 vCPU and 16 GB RAM, and is the default
- “Enterprise” is 16 vCPU and 96 GB RAM

Deployment on VMware hypervisors

- Import the OVA file
- Deploy the OVF package (OVA file)
 - In VMware Workstation Pro/Player, deploy a new virtual machine
 - Otherwise, deploy an OVF template by using vSphere Client
- Power on the virtual gateway in hypervisor
- Map Ethernet interfaces
 - If this step is omitted during the virtual gateway deployment
 - Might require VMware administrator assistance
- Configure the virtual gateway
 - Modify CPU, memory, and hard disk from deployment settings
- Initialize the virtual gateway
 - Same as for physical gateways

Figure 1-11. Deployment on VMware hypervisors

Virtual gateways for Citrix XenServer hypervisor

Delivered as a .tar file

- Naming convention:
 - xxx.prod.vhd.tar (Production edition)
 - xxx.nonprod.vhd.tar (Nonproduction edition)
- After unpacking, the resulting files are:
 - dpxenmgmt.sh script for CLI-based deployment
 - xxx.vhd.gz file that contains the compressed VHD file (firmware and configuration data)
- Minimum resource allocation:
 - Without API workload, 4 vCPU and 4 GB RAM
 - Developers edition: 2 vCPU and 4 GB RAM
 - With API workload, 4 vCPU and 8 GB RAM

Figure 1-12. Virtual gateways for Citrix XenServer hypervisor

The prefix in the TAR file name varies with the firmware version.

Deployment on Citrix XenServer hypervisors

- Deployment can be performed by using the XenServer GUI or CLI commands
 - CLI is preferred for performance reasons
- Deploy the VHD package
 - Unpack the .tar file
- Use the dpxenmgmt.sh script and parameters to deploy and start the virtual gateway
 - vCPU
 - RAM
 - RAID drive size, resize
 - Networking

Figure 1-13. Deployment on Citrix XenServer hypervisors

Virtual gateways for Linux

- Delivered as Debian files (Ubuntu) or RPM files (RHEL)
 - 64 bit Linux required
- Ubuntu:
 - xxx.common_amd64.deb, xxx.image_amd64.deb
 - Use **dpkg** command to install
- RHEL
 - xxx.image.x86_64.rpm, xxx.common.x86_64.rpm
 - Use **yum install** to install
- Minimum resource allocation:
 - Without API workload, 4 vCPU and 4 GB RAM
 - Developers edition: 2 vCPU and 4 GB RAM
 - With API workload, 4 vCPU and 8 GB RAM

Figure 1-14. Virtual gateways for Linux

The prefix in the DEB and RPM file names vary with the firmware version.

Deployment on Linux

- `/opt/ibm/datapower/datapower.conf` used for some configuration
 - Number of CPUs
 - Upper limit of memory that DataPower can use
 - “config” and “local” file directory locations on Linux
 - Location of RAID device (image file or block device)
- DataPower runs as *root*
- DataPower is controlled by:
 - The **initctl** command in Ubuntu
 - The **systemctl** command in RHEL
- DataPower inherits or uses some configuration from the Linux host:
 - DNS, host name, Time and date, network interfaces, host aliases
- Although DataPower for Linux can run under a Linux inside a Docker container, it is easier and more efficient to use DataPower Gateway for Docker directly

[DataPower deployment environments](#)

© Copyright IBM Corporation 2018

Figure 1-15. Deployment on Linux

The prefix in the DEB and RPM file names vary with the firmware version.

DataPower assumes that it is the only application that is running on Linux. The “upper memory limit” can be used to keep DataPower from using all of Linux memory, which allows other applications to execute.

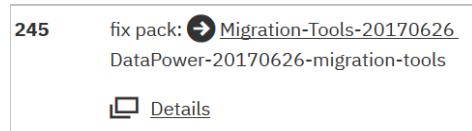
Network interfaces for virtual gateways

- The **physical** IBM DataPower Gateway has 12 Ethernet interfaces
- Number of network interfaces for a **virtual** gateway depends on the hosting environment:
 - VMware and Citrix
 - eth0, eth1, eth2, eth3
 - Speeds depend on hypervisor and hardware
 - Physical mode and flow control settings are ignored
 - VMware under IBM PureApplication System
 - Only eth1-eth3 are available to the gateway
 - eth0 is used by IBM PureApplication System management
 - Linux
 - The gateway “discovers” the available network interfaces during startup
 - Host aliases are created for the discovered interfaces – `ethernetInterface_IPversion_n` (example is `eth0_ipv4_1`)
 - Docker
 - Similar to Linux – DataPower Docker container “discovers” available host interfaces upon startup

Figure 1-16. Network interfaces for virtual gateways

Migrating a virtual XI or XG to a virtual IDG

- DataPower V7.6.0 does **not** provide firmware for virtual XI52 or XG45 gateways
 - IBM Support Technote (in 7.6 Removed Features table)
<http://www.ibm.com/support/docview.wss?uid=swg21634531>
- You must use the provided migration tool to convert the virtual XI/XG gateway to a IBM DataPower Gateway (IDG)
- The migration tool is found on Fix Central
 - Search on *Installed Version of ALL* (not a specific firmware version)
 - In the resulting large list, *Search on the text migration*



- The *Details* link takes you to the Technote that contains the migration procedure

Figure 1-17. Migrating a virtual XI or XG to a virtual IDG

The migration tool is found on the IBM Fix Central support site at:

<https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm%7EWebSphere&product=ibm/WebSphere/WebSphere+DataPower+SOA+Appliances&release>All&platform>All&function=textSearch&text=migration>

DataPower in the cloud

When DataPower runs in the cloud, it is running under a hypervisor, in Linux, or in a Docker container

- DataPower in a Docker container is supported in:
 - IBM Cloud
 - Amazon Web Services (AWS)
 - Google Cloud
 - Microsoft Azure
- DataPower Virtual Edition is supported in:
 - PureApplication System W1500 or W2500 V2.0
 - PureApplication Service on SoftLayer with x86 hardware
 - SoftLayer bare metal instances that use supported hypervisors
 - SoftLayer CCI
 - Amazon EC2 virtual server
 - Microsoft Azure virtual server

Figure 1-18. DataPower in the cloud

“IBM Cloud” previously named “IBM Bluemix”.

For SoftLayer, “CCI” is a “CloudLayer Computing Instance”

Downloading DataPower Gateway for Developers on Docker

- Docker

- <https://docker.hub.com>

- Search on “ibmcom/datapower”

- Use this official IBM version



- IBM Fix Central (<https://www.ibm.com/support/fixcentral/>)

- The download file (tar.gz) is under the firmware

- Example: V7.6.0.2 firmware

- [idg_docker7602.tar.gz](#)

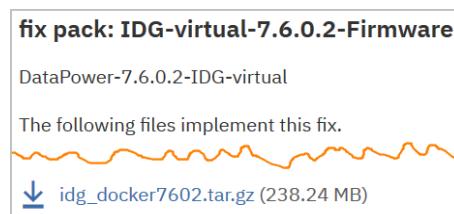


Figure 1-19. Downloading DataPower Gateway for Developers on Docker

To run the DataPower Gateway in a Docker container, run the Docker image that contains the DataPower Gateway.

The image requires a minimum of 4 GB RAM and 2 CPUs.

DataPower Gateway for Developers runs on Docker Engine V1.12 or later.

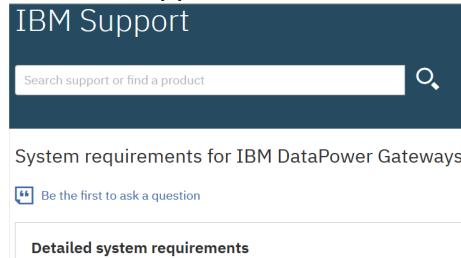
Certain functions are unavailable or follow the Docker conventions when the DataPower Gateway runs in a Docker container.

- You cannot configure Ethernet interfaces, VLAN interfaces link aggregation interfaces, and network settings. All commands are unavailable.
- You cannot configure the NTP service. All commands are unavailable.
- You cannot configure a Secure Gateway client. All commands are unavailable.
- You cannot set the date or time. The clock command is unavailable.

DataPower Software Product Compatibility Reports: 1 of 2

A Software Product Compatibility Report (SPCR) identifies what products and versions are officially supported

- Starting point for DataPower
 - <http://www.ibm.com/support/docview.wss?uid=swg27040227>



The screenshot shows the IBM Support website interface. At the top, there is a search bar with the placeholder "Search support or find a product" and a magnifying glass icon. Below the search bar, the text "System requirements for IBM DataPower Gateways" is displayed. Underneath this text, there is a button labeled "Be the first to ask a question". At the bottom of the visible area, there is a link labeled "Detailed system requirements".

- Further down the page, select the appropriate firmware version



Figure 1-20. DataPower Software Product Compatibility Reports: 1 of 2

See the system requirements for IBM DataPower Gateways at
<http://www.ibm.com/support/docview.wss?uid=swg27040227>

DataPower Software Product Compatibility Reports: 2 of 2

- After a version is selected, the supported DataPower products for that version are listed

7.6.0	7.5.2	7.5.1	7.5	7.2	7.1
Requirements by product					
DataPower Gateway	Production and Nonproduction Edition of DataPower Gateway	Developers Edition of DataPower Gateway Virtual Edition			
DataPower Service Gateway (XG45)	Virtual Edition				
DataPower Integration					

- Select the product of interest
 - For this example, the “Production and Nonproduction Edition of the Virtual Edition” is selected

Figure 1-21. DataPower Software Product Compatibility Reports: 2 of 2

The system requirements are listed by deployment type within version number.

Differences in capabilities in the deployment options

- Physical appliances are equipped with physical disks for storing auxiliary data
- The available add-on modules and features differ on different platforms
 - Physical appliance includes the tenant module
 - Tenant module enables multiple DataPower versions to run on the same physical appliance
 - Can be useful if you want to limit the upgrades that are required on the production tenant while including a newer version for some applications like API Connect
- Scaling deployment
 - With physical and virtual appliances, you scale deployments by adding additional DataPower Gateway instances to a tier of load balanced DataPower Gateway instances
 - DataPower on Docker uses Docker container orchestration for controlling a tier of containers
- Refer to the IBM Knowledge Center for DataPower Gateways
 - See the section titled “Differences among DataPower Gateways products”

Figure 1-22. Differences in capabilities in the deployment options

For more information, see

https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/differencesamongproducts.html

Unit summary

- Identify the different editions of the Virtual Edition, and how they differ
- Describe the DataPower deployment options
- List some of the physical characteristics of the DataPower hardware
- Describe the Ethernet interface options for the physical and virtual gateway
- List the supported runtime environments for the Virtual Edition
- List the basic steps for deploying a virtual gateway in the VMware, Citrix, Linux, and Docker environments
- List the supported cloud environments for the virtual gateway
- Describe the Docker support for DataPower
- Describe how to request and use a Software Product Compatibility Report

Figure 1-23. Unit summary

Review questions

1. **True or False:** Certain functions are unavailable or follow the Docker conventions when the DataPower Gateway runs in a Docker container.
2. Which of these environments does NOT support the IBM DataPower Gateway?
 - A. Xen.
 - B. VMware.
 - C. Windows Hyper-V.
 - D. Linux.

Figure 1-24. Review questions

Write your answers here:

1.

2.

Review answers

1. **True.** Certain functions are unavailable or follow the Docker conventions when the DataPower Gateway runs in a Docker container. The networking is controlled by Docker.
2. **C.** Which of these environments does NOT support the IBM DataPower Gateway?
C. Windows Hyper-V.

Figure 1-25. Review answers

Unit 2. Initial setup

Estimated time

01:15

Overview

This unit introduces you to the initial process of setting up the DataPower appliance. It covers both physical and virtual appliances. You learn how to use the serial interface to connect to the CLI interface to complete the initial box setup. You also learn about some of the other appliance settings.

How you will check your progress

- Review questions

References

IBM DataPower Gateways 7.6.0 Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0

Unit objectives

- Describe how to start the DataPower Gateway on the various deployment types
- Identify the Ethernet connections for physical and virtual appliances
- Use the console connector or console view for initial configuration
- Deploy a virtual appliance on various hypervisors
- Describe the minimal steps that are done during the initial configuration
- Access the Web Management graphical interface
- Configure the Ethernet interfaces for an appliance
- Configure RBM, DNS, NTP, and System Settings
- Configure user interface settings
- Prepare the appliance auxiliary storage
- Enable support for other languages for the Web Management graphical interface logs and messages

Initial setup

© Copyright IBM Corporation 2018

Figure 2-1. Unit objectives

Starting a gateway

The way to start a DataPower gateway depends on the deployment platform

- Physical gateway – power on the physical device
- Virtual gateway under a VMware hypervisor – power on the virtual machine
- Virtual gateway under a Citrix hypervisor – run the `dpxenmgmt.sh` script
- Virtual gateway in Linux – run the `datapower-launch` command
- Virtual gateway from DataPower Gateway for Developers – run the `docker run` command

Initial setup

© Copyright IBM Corporation 2018

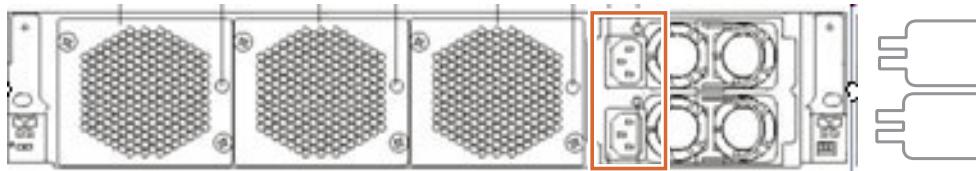
Figure 2-2. Starting a gateway

The way that you start the DataPower Gateway appliance depends on whether the form factor is physical, virtual, Linux, or Docker.

Starting a DataPower physical gateway

- Before turning on the power switch, connect *both* power supply modules to AC power by using the cables that were included with the gateway
 - You must connect both power supply modules to AC power
 - Otherwise, the gateway firmware considers the unconnected module to be in a failed state
- Wait for a few seconds until the gateway starts and the `login:` prompt opens on the serial console
- Default login “root” account is **admin**, and the initial password is **admin**
 - **admin** is a “privileged user” account

```
Welcome to DataPower Gateway console configuration.
Copyright IBM Corporation 1999-2016
Version: IDG.7.6.0.x buildx.xx on y/m/d h:m:s
Serial number: xxxxxxxxxxxx
Unauthorized access prohibited.
login:
```



Initial setup

© Copyright IBM Corporation 2018

Figure 2-3. Starting a DataPower physical gateway

Ensure that IBM cables are being used to connect to the power source. Upon installation, the default user name and password are set to: **admin** and **admin**

After the initial login, you are prompted to provide a new password for the admin account.

Starting a DataPower virtual gateway

- Depends on the particular environment: hypervisor, Linux
- Wait for a few seconds until the virtual gateway starts
- Switch to the console view in the environment
- The same `login:` prompt that appears for physical gateways also opens for virtual gateways
- Default login “root” account is **admin**, and the initial password is **admin**
 - **admin** is a “privileged user” account

```
Welcome to DataPower Gateway console configuration.  
Copyright IBM Corporation 1999-2016  
Version: IDG.7.6.0.x buildx.xx on y/m/d h:m:s  
Serial number: xxxxxxxxxxxx  
Unauthorized access prohibited.  
login:
```

- For DataPower on Docker:
 - The `login:` prompt is presented before the banner information is displayed
 - The DataPower console and the DataPower system log entries are interspersed

Figure 2-4. Starting a DataPower virtual gateway

After you start the DataPower Gateway, a login prompt is displayed in the CLI.

The initial account is **admin** and the initial password is **admin**.

Initializing or reinitializing the gateway (1 of 2)

```
Please enter new password: xxxxxxxx  
Please re-enter new password to confirm: xxxxxxxx  
Do you want to run the Installation Wizard? y
```

- Enter a new password at the **Please enter new password** prompt
- If you want initial configuration prompts, enter **y** at the **Do you want to run the Installation Wizard?** prompt
- Follow the prompts to complete the base configuration:
 - Network interfaces
 - DNS server
 - Unique system identifier
 - Web management and SSH management
 - Credentials for an account that can reset passwords
 - RAID volume
- If you are not able to complete the initialization, you can use the **startup** command at any time to start the Installation wizard
 - The **startup** command is not available when running directly under Linux

Figure 2-5. Initializing or reinitializing the gateway (1 of 2)

The base configuration can be defined from individual command entries, prompts from the installation wizard during the initial boot sequence, or with the **startup** command. The **startup** command starts the Installation Wizard.

The **reinitialize** CLI command deletes all configuration data and restarts the gateway. All user accounts (except for **admin**), passwords, domains (except for **default**), services, and network configuration are deleted. Only the serial interface for CLI is available.

Initializing or reinitializing the gateway (2 of 2)

- You are prompted about selecting two operational modes:
 - Disaster recovery mode
 - Common Criteria compatibility mode
- These modes can be set only at the initial boot, or during a reinitialization
- Enabling disaster recovery mode allows the use of secure backup and secure restore
 - Copies the gateway configuration, files, certificates, and private keys to an encrypted backup file
- Enabling Common Criteria compatibility mode applies settings and policies that conform to Common Criteria requirements (EAL4)
 - Sets properties like minimum length for passwords
 - Set only if this mode is required to conform to the EAL4 standard
 - Read the section “When to use Common Criteria Compatibility mode” in the IBM Knowledge Center for further details

Initial setup

© Copyright IBM Corporation 2018

Figure 2-6. Initializing or reinitializing the gateway (2 of 2)

“EAL4” is Evaluation Assurance Level 4 of the Common Criteria standard.

If you are unsure about whether to use Common Criteria Compatibility mode, you most likely do not. In general, Common Criteria is only used when a specific authority requires that the DataPower Gateway needs to be EAL4 certified. Without this specific requirement, select no during initialization.

Administration by using the command-line interface

- The command-line interface (CLI) provides a text terminal for administering the DataPower Gateway
 - In the initial setup, you must enable the Web Management graphical application and Ethernet ports with the CLI through a serial connection (console connector for a physical gateway, and Console tab for a virtual gateway)
 - Administrators have the option of enabling the CLI over a Telnet or Secure Shell (SSH) connection

```
susehost:~ # ssh 172.16.79.123
DP #12
Unauthorized access prohibited.
login: admin
Password: *****
```

[Initial setup](#)

© Copyright IBM Corporation 2018

Figure 2-7. Administration by using the command-line interface

For security purposes, the CLI was not designed to be a generic command shell environment. Its purpose is strictly limited to the configuration and administration of the DataPower Gateway Appliance. It is a powerful interface that has access to all services and interfaces on the gateway itself.

By default, the DataPower Gateway Appliance is packaged with all the Ethernet interfaces disabled. To activate the ports, you must enable the interfaces within the CLI over a serial port connection. Similarly, the WebGUI administration web application must also be enabled before use.

When the DataPower Gateway Appliance is properly configured, you can allow Telnet or Secure Shell connections to the CLI.

The CLI is a streamlined yet powerful system for controlling every facet of the gateway. Although it looks like a command shell, there is no compiler or interpreter to run arbitrary code. The `alias` function is a macro for multiple CLI commands, and the `exec` function runs configuration scripts that are limited to the gateway itself.

In the global configuration mode, the administrator can create, modify, or remove any DataPower service or interface that can be found in the Web Management graphical interface.

Initial CLI login screen

```

login: admin          1
Password: *****

Welcome to DataPower XI52 console configuration.
Copyright IBM Corporation 1999-2014
Version: xi52.7.0.x.x build yyyyyy on 2014/zz/zz 10:28:06
Serial number: 6XXXXXXX

xi52# show system    2
  description: DataPower XI52
  serial number: 6XXXXXXX
  entitlement id: 6XXXXXXX
    product id: 5725 [Rev None]
    OID: 1.3.6.1.4.1.14685.1.3
    uptime: 5 days 20:59:01
    contact: Jim Brown/Los Angeles
    name: DP #10
    location: IBM WebSphere Education Dublin DataPower #10
    services: 72
  backup mode: secure
  product mode: normal
  audit-reserve: 40 kBytes

```

Initial setup

© Copyright IBM Corporation 2018

Figure 2-8. Initial CLI login screen

After defining the base firmware configuration, the screen displays information that is similar to the following information. The screen shows information specific to your gateway.

1. You must provide a valid user login ID and password to access the command-line interface.
2. The initial welcome message lists the firmware build level and date, and the serial number of the DataPower gateway. The serial number for a virtual gateway is 0000000.
3. Use the `show` command to show system information about the interfaces, objects, and the gateway itself.

Quick initial configuration procedure

- Sample CLI commands to configure an Ethernet interface, WebGUI, and CLI over SSH

```

xi52# configure terminal 1
Global configuration mode
xi52(config)# ethernet eth10 2
Modify Ethernet Interface configuration
xi52(config ethernet eth10)# ip-address 10.0.0.1/8 3
xi52(config ethernet eth10)# exit 4
xi52(config)# web-mgmt 10.0.0.1 9090 3600 5
Web management: successfully started
xi52(config)# ssh 10.0.0.1 22 6
%       Pending

SSH service listener enabled
xi52(config)# write memory 7
Overwrite previously saved configuration? [y/n]:y
Configuration saved successfully
xi52(config)# exit 8

```

Initial setup

© Copyright IBM Corporation 2018

Figure 2-9. Quick initial configuration procedure

After logging in to the DataPower Gateway Appliance for the first time over a serial connection, do these steps to enable the WebGUI administration web application over the management port (`mgt0`).

1. While logged in as the administrator, enter the global configuration mode.
2. Configure an Ethernet interface (`eth10`), entering the Ethernet configuration mode.
3. Assign a static IP address and a subnet mask (CIDR notation) for the Ethernet interface.
4. Exit the Ethernet configuration mode.
5. In the global configuration mode, enable the WebGUI administration application (`web-mgmt`), assign it to port 9090, and set the session idle timer to 3600 seconds.
6. Enable the SSH CLI access on port 22.
7. Save the current configuration to the file system.
8. Exit the global configuration mode.

Accept the license agreement by using the WebGUI

Upon initialization, the administrator must access the Web Management graphical interface and accept the license agreement. Some of the base configuration cannot be completed (such as the XML management service) until the license is accepted.

The following steps are required:

1. Open the web browser
2. In the **Address** field, enter `https://<datapower_address>:<WebGUI_port>`
 - a. If the web page is displayed successfully, the base firmware configuration is successful
3. Enter the local administrator account and password
4. Click **Login**
 - a. The WebGUI displays the license agreement
 - b. Click **I agree** to accept the terms of the license agreement and non-IBM-terms
 - c. The gateway reloads the firmware and in a few minutes, the administrator can log in again after the gateway restarts
 - d. If the administrator does not agree, click **I do not agree** and the initialization of the gateway stops
 - e. The administrator needs either to power off the gateway or to review and accept the license agreement
5. Log in again to verify that the admin account and other administrators can access the gateway with their credentials

Figure 2-10. Accept the license agreement by using the WebGUI

Upon initialization, the administrator must access the Web Management graphical interface and accept the license agreement. Some of the base configuration cannot be completed (such as the XML management service) until the license is accepted.

[Initial setup](#)

© Copyright IBM Corporation 2018

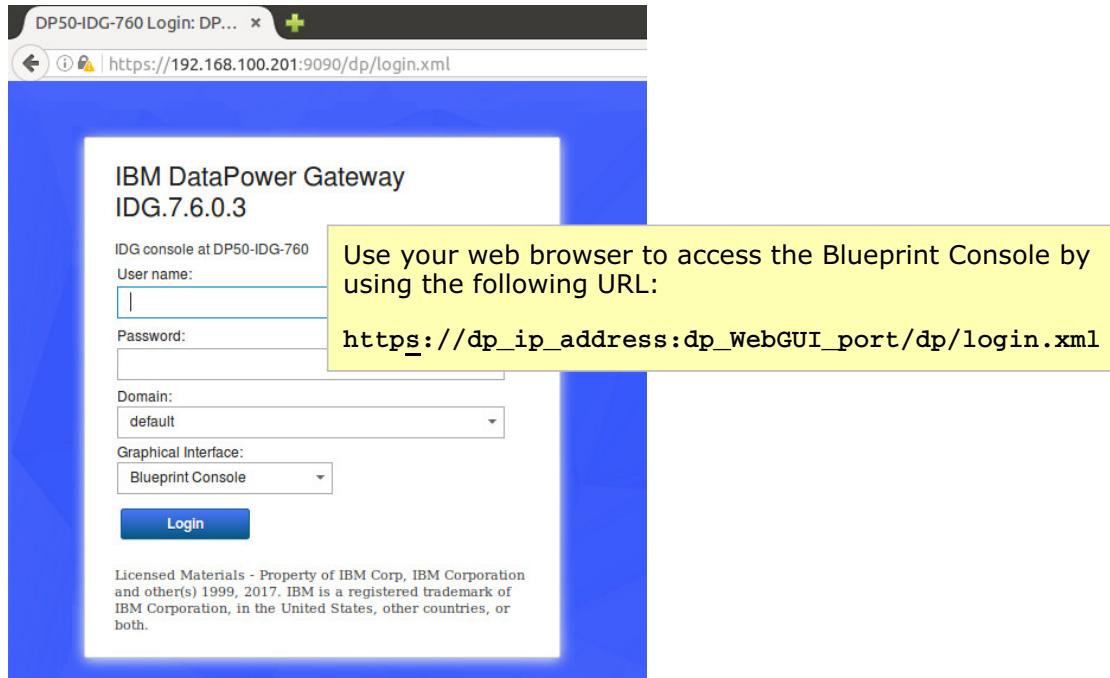
Figure 2-11. Access the WebGUI

The string `dp_ip_address` in the URL is the IP address that the Web Management Service listens on. The string `dp_WebGUI_port` is the TCP port number that is assigned to the WebGUI application. The default value is 9090.



Access to the Blueprint Console

- The Blueprint Console is the newer Web Management interface



Initial setup

© Copyright IBM Corporation 2018

Figure 2-12. Access to the Blueprint Console

The string `dp_ip_address` in the URL is the IP address that the Web Management Service listens on. The string `dp_WebGUI_port` is the TCP port number that is assigned to the Web Management service. The default value is 9090.

When the suffix `/dp/login.xml` is added, the sign-on defaults to the Blueprint Console graphical interface.

The Blueprint Console and the WebGUI contain the same management features. The difference is in the layout and navigation of the web pages.

The WebGUI is deprecated in DataPower Gateway V7.6.



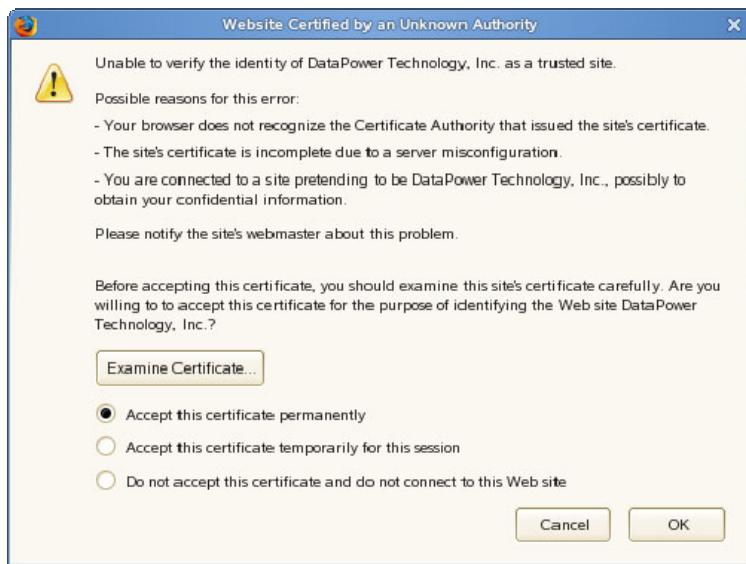
Information

Many of the screen captures that you see in the presentation units are taken from the WebGUI graphical interface.

The instructions for the exercises that accompany this course use the Blueprint Console navigation and page layout in the screen captures.

Web management graphical interface certificate error

- Connect to the WebGUI by using HTTP and SSL (HTTPS)
 - The DataPower gateway includes a digital certificate that is used during SSL communication
 - The common name in the certificate is *DataPower WebGUI*



Initial setup

© Copyright IBM Corporation 2018

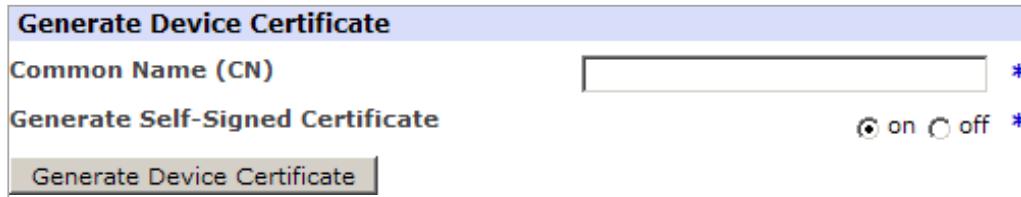
Figure 2-13. Web management graphical interface certificate error

The first time that you access the DataPower GUI login page, you receive a warning that your connection is not secure and that the page uses an invalid security certificate. Depending on the browser that you are using, you can accept the certificate or you can click the Advanced button in the browser and add the exception to continue to the DataPower GUI login page.

- A warning occurs because the domain name where the gateway is hosted does not match the common name inside the digital certificate
- Safely ignore the warning to continue to the DataPower GUI login page

Generate a gateway certificate

- Generate a gateway certificate for your gateway to fix a “Domain Name Mismatch” security warning
- In the **System Control** panel, enter the **Common Name (CN)** for the certificate
 - Must associate the certificate with the custom SSL proxy profile for the web management service



- The generate device certificate for the DataPower Gateway procedure is deprecated
 - Use the Crypto Tools key generation action to create a private cryptographic key and optionally a self-signed certificate for the Gateway

[Initial setup](#)

© Copyright IBM Corporation 2018

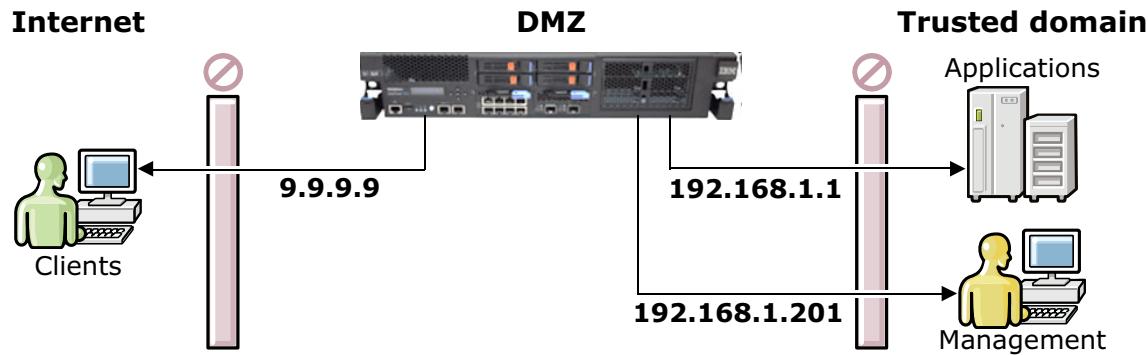
Figure 2-14. Generate a gateway certificate

The **Generate Self-Signed Certificate** flag enables the self-signing of the certificate. Otherwise, a certificate authority must sign this digital certificate. Check with your security administrators or security policy to determine the action to take with this certificate.

This procedure is deprecated. Instead, use the Crypto Tools key generation action to create a private cryptographic key and optionally a self-signed certificate for the DataPower Gateway.

You get to use the Crypto Tools key generation action in a later exercise.

Typical interface topology



Isolate network traffic to separate the network segments.

- Management interface: Responsible for all management traffic
 - SSH, WebGUI, SNMP, failure notification (SMTP), and off-device logging (syslog)
- Connect one interface to an external facing switch or router to handle *external* traffic
 - Traffic entering through the DMZ
- Connect another interface to an internal switch or router for *internal* traffic
 - Traffic entering through internal networks

Assign each Ethernet interface with an IP address, default gateway, static routes, and more.

[Initial setup](#)

© Copyright IBM Corporation 2018

Figure 2-15. Typical interface topology

On physical appliances there are two management ports, mgt0 and mgt1, and up to 10 Ethernet ports.

Defining Ethernet interfaces in the WebGUI

- Control Panel > Network > Interface > Ethernet Interface
- The number of available interfaces depends on the particular gateway model

The screenshot shows two panels of the IBM WebGUI interface:

- Left Panel (Configure Ethernet Interface):**
 - Header: "Configure Ethernet Interface".
 - Tab navigation: Main (selected), Standby control, Advanced.
 - Ethernet Interface: eth0 [up] (highlighted with a red arrow).
 - Buttons: Apply, Cancel, Delete, Undo.
 - Section: Basic configuration. Sub-section: Administrative state. Options: enabled (radio button selected) and disabled.
- Right Panel (Configure Ethernet Interface):**
 - Header: "Configure Ethernet Interface".
 - Link: Refresh List.
 - Table:

Name	Status	Op-State	Logs	Administrative state	Comments
eth0	saved	up		enabled	
eth1	saved	up		enabled	
eth2	saved	up		enabled	
eth3	saved	up		enabled	

© Copyright IBM Corporation 2018

Figure 2-16. Defining Ethernet interfaces in the WebGUI

Virtual appliances have eth0, eth1, eth2, and eth3 interfaces.

Defining a specific Ethernet interface: Main tab

- Address configuration mode:
 - Static, DHCP, and SLAAC
- Primary and secondary IP addresses, and subnet mask
- Default gateway
- Static routes

Basic configuration Administrative state <input checked="" type="radio"/> enabled <input type="radio"/> disabled Comments IP address configuration mode <input checked="" type="checkbox"/> Static <input type="checkbox"/> DHCP <input type="checkbox"/> SLAAC Enable for link aggregation <input type="radio"/> on <input checked="" type="radio"/> off							
IP addressing Primary IP Address <input type="text" value="172.16.78.11/16"/> Secondary Addresses <input type="text" value="(empty)"/> <input type="button" value="add"/>							
IP routing Default IPv4 gateway <input type="text" value="172.16.79.1"/> <input type="button" value="Ping"/> Default IPv6 gateway <input type="text"/> Static routes <table border="1"> <thead> <tr> <th>Destination</th> <th>Next-hop router</th> <th>Metric</th> </tr> </thead> <tbody> <tr> <td colspan="3">(empty)</td> </tr> </tbody> </table>		Destination	Next-hop router	Metric	(empty)		
Destination	Next-hop router	Metric					
(empty)							

Initial setup

© Copyright IBM Corporation 2018

Figure 2-17. Defining a specific Ethernet interface: Main tab

SLAAC is “Stateless address autoconfiguration”, a dynamic addressing scheme for IPv6.

Subnet masks are in CIDR (Classless Inter-Domain Routing) notation.



DNS settings

- **Control Panel > Network > Interface > DNS Settings**

- **Search domains**

- To resolve partial host names

- **DNS servers**

- **Static hosts**

- Predefined host name to IP address resolution

- **Load-balancing algorithm**

- How to select which DNS server to use

- “Round robin” or “first alive”

Administrative state	<input checked="" type="radio"/> enabled <input type="radio"/> disabled												
Comments	<input type="text"/>												
IP preference	IPv4 <input type="button" value="▼"/>												
Search domains	<table border="1"> <tr> <td>Domain name</td> <td><input type="text"/></td> </tr> <tr> <td>(empty)</td> <td><input type="button" value="Add"/></td> </tr> </table>	Domain name	<input type="text"/>	(empty)	<input type="button" value="Add"/>								
Domain name	<input type="text"/>												
(empty)	<input type="button" value="Add"/>												
DNS servers	<table border="1"> <thead> <tr> <th>IP address</th> <th>UDP port</th> <th>TCP port</th> <th>Attempts</th> </tr> </thead> <tbody> <tr> <td>172.16.79.1</td> <td>53</td> <td>53</td> <td>3</td> </tr> <tr> <td>172.16.79.2</td> <td>53</td> <td>53</td> <td>3</td> </tr> </tbody> </table>	IP address	UDP port	TCP port	Attempts	172.16.79.1	53	53	3	172.16.79.2	53	53	3
IP address	UDP port	TCP port	Attempts										
172.16.79.1	53	53	3										
172.16.79.2	53	53	3										
Static hosts	<table border="1"> <thead> <tr> <th>Host name</th> <th>IP address</th> </tr> </thead> <tbody> <tr> <td>(empty)</td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Host name	IP address	(empty)	<input type="button" value="Add"/>								
Host name	IP address												
(empty)	<input type="button" value="Add"/>												
<input type="button" value="Load balancing algorithm"/> <input type="button" value="Round robin"/> *													

Initial setup

© Copyright IBM Corporation 2018

Figure 2-18. DNS settings

The example shows the navigation and screen settings for the WebGUI.

From the Blueprint Console, select the Network icon. Then, select Interface > DNS Settings.



Time and date settings

- Manually enter in **Control Panel > Administration > Main > System Control**

Or,

- Point to the NTP server in **Control Panel > Network > Interface > NTP Service**

NTP Service [up]

Administrative state: enabled disabled

Comments: [empty text field]

NTP server:

Refresh interval: Sec

Initial setup © Copyright IBM Corporation 2018

Figure 2-19. Time and date settings

You can change the date and time values manually from the Administration > Main > System Control page.

Alternatively, use specify an internal or external NTP server to synchronize the date of the appliance.

Configure management services

- Management services:
 - Telnet Service
 - SSH Service
 - Web Management Service
 - XML Management Interface
 - REST Management Service



- Configure the **Local IP Address** of the management service to restrict access through the management interface only
 - If you use the IP address **0.0.0.0** it allows traffic through any Ethernet interface

Web Management Service [up]	
Admin State	<input checked="" type="radio"/> enabled <input type="radio"/> disabled
Local IP Address	192.168.0.25
Port Number	8080

Initial setup

© Copyright IBM Corporation 2018

Figure 2-20. Configure management services

The Telnet service is not recommended because it transmits the CLI commands unencrypted.

During an gateway's initial configuration, CLI commands typically configure and start the SSH service and the web management service (WebGUI).

The local IP address that is assigned to the web management interface allows only traffic from the Ethernet interface that is configured with that IP address.

In this example, the WebGUI can be accessed by using the IP address 192.168.0.25, although other Ethernet interfaces might be configured.



Set basic RBM settings: Password policy tab

- Administration > Access > RBM Settings

- Password length
- Require mixed case
- Require non-alphanumeric
- Require number
- Disallow a user name as part of the password
- Have password expire
- Control reuse of the password

Minimum length	<input type="text" value="6"/>
Require mixed case	<input type="radio"/> on <input checked="" type="radio"/> off *
Require non-alphanumeric	<input type="radio"/> on <input checked="" type="radio"/> off *
Require number	<input type="radio"/> on <input checked="" type="radio"/> off *
Disallow user name substring	<input type="radio"/> on <input checked="" type="radio"/> off *
Enable aging	<input type="radio"/> on <input checked="" type="radio"/> off *
Control reuse	<input type="radio"/> on <input checked="" type="radio"/> off *
Password hash algorithm	<input type="text" value="md5crypt"/> <input type="button" value="▼"/>

Initial setup

© Copyright IBM Corporation 2018

Figure 2-21. Set basic RBM settings: Password policy tab

RBM means “role-based management.”

RBM is covered in a later unit.

Set password rules as dictated by the site password policy.

Set basic RBM settings: Account policy tab

- Administration > Access > RBM Settings

- Restrict the **admin** login to the serial port only
- When and how long to lock an account for failed password attempts
- Whether to enforce RBI rules on CLI
- CLI idle timeout

Restrict admin to serial	<input type="radio"/> on <input checked="" type="radio"/> off
Maximum failed logins	<input type="text" value="0"/> *
Lockout duration	<input type="text" value="1"/> Minutes
Enforce RBM on CLI	<input checked="" type="radio"/> on <input type="radio"/> off
CLI idle timeout	<input type="text" value="0"/> Seconds *

Initial setup

© Copyright IBM Corporation 2018

Figure 2-22. Set basic RBM settings: Account policy tab

You can set the maximum number of failed login attempts before a lockout is enforced. Use “0” failed logins to **not** enforce this restriction.

A lockout duration of “0” indicates a permanent lockout. The **admin** account cannot be permanently locked out; a “0” value causes the lockout to be 120 minutes.

An administrator account (privileged user) can re-enable locked accounts.



Configure system settings

- Administration > Device > System Settings

Initial setup

Description	DataPower XI52
Serial number	0000000
Entitlement serial number	0000000
Product ID	5725 [Rev None]
Contact	Jim Brown/Los Angeles
Appliance name	DP98
Location	Dublin
Services	72
Backup mode	Secure backup with keys and certif
Product Mode	Normal
Custom user interface file	local:///
	(none) <input type="button" value="Upload..."/> <input type="button" value="Fetch.."/>

© Copyright IBM Corporation 2018

Figure 2-23. Configure system settings

Entitlement Number is the serial number of the gateway, as shown in the **Serial Number** field, if this installation is the original installation of the gateway. If the gateway was replaced because of a repair, this field contains the serial number of the original gateway; it is used for future maintenance or warranty service.

The serial number for a virtual gateway is 000000.

Contact, **Appliance name**, and **Location** are text fields that are displayed for a `show system` CLI command. The Appliance name is also displayed on the header of the WebGUI page.

Custom User Interface File is a reference to an XML file that defines customized messages that are displayed in the WebGUI or a CLI session.

Create a secondary administrative account

- An effective process is to create a second administrative account to distribute to administrators
 - Keeps the root **admin** account and password confidential
 - Provides “backup” to the **admin** account
- The Initialization wizard prompts you to create one
 - Otherwise, create one on your own
- **Administration > New user account**
 - Do not restrict to a specific domain
 - Select **System administrator**
 - Assigns the account to the predefined **sysadmin** user group
- Also, add CLI command groups to the sysadmin user group
 - Allows the secondary administrative account to also enter CLI commands in an SSH session

Figure 2-24. Create a secondary administrative account

Generally, if you lose the **admin** account password, and have no other administrative backup account, you must return the gateway to DataPower Support for resetting.

Custom user interface file

An XML file where custom text is added to certain parts of the Web Management service and CLI.

- WebGUI
 - A pre-login message that displays before a user logs in
 - A post-login message that displays in a pop-up window immediately after users log in
 - System messages that can be displayed on the top of the page, the bottom of the page, or in both locations
- CLI
 - A pre-login message that displays before a user logs in
 - A post-login message that displays immediately after users log in
 - A system message that displays after each command invocation

Documented in the IBM Knowledge Center.

Validate the user interface XML file against the user interface schema by using the *test schema* CLI command.

Figure 2-25. Custom user interface file

The schema of the user interface XML file is defined: `store:///schemas/dp-user-interface.xsd`

The test schema CLI command format is: `test schema XML_file_url schema_url`

Custom user interface file: WebGUI example

- <MarkupBanner type="pre-login" foreground-color="blue" background-color="yellow">
WebGUI pre-login message
</MarkupBanner>

WebSphere DataPower Login

XI52 console at DP #15

WebGUI pre-login message

User Name:

- <MarkupBanner type="post-login" foreground-color="blue" background-color="yellow">
WebGUI post-login pop up message
</MarkupBanner>

Post Login Message - Windows Inte...

https://w... Ce...

WebGUI post-login pop up message

- <MarkupBanner type="system-banner" location="header" foreground-color="green" background-color="red">
WebGUI system message-header
</MarkupBanner>

WebGUI system message-header

WebSphere. DataPower XI52

Control Panel

Pattern Console

Figure 2-26. Custom user interface file: WebGUI example

The complete XML syntax includes the User-Interface tag. On the next page, you see the complete banner.xml file that is used for this demonstration.



Syntax

<User-Interface

```
xmlns="http://www.datapower.com/schemas/user-interface/1.0">
<!!-- Markup for custom messages for the WebGUI interface -->
<MarkupBanner type="pre-login" foreground-color="blue"
background-color="yellow">
WebGUI pre-login message
</MarkupBanner>
<MarkupBanner type="post-login" foreground-color="blue" background-color="yellow">
WebGUI post-login pop up message
</MarkupBanner>
<MarkupBanner type="system-banner" location="header" foreground-color="green"
background-color="red">
WebGUI system message - header
</MarkupBanner>
<MarkupBanner type="system-banner" location="footer" foreground-color="blue"
background-color="yellow">
WebGUI system message - footer
</MarkupBanner>
<!!-- Markup for custom messages for the interface -->
<TextBanner type="pre-login">
pre-login message
</TextBanner>
<TextBanner type="post-login">
post-login message
</TextBanner>
<TextBanner type="system-banner">
system message
</TextBanner>
</User-Interface>
```

Custom user interface file: CLI example

- ```
<TextBanner type="pre-login">
 pre-login message
</TextBanner>
```

Unauthorized access prohibited.

**pre-login message**

login:

- ```
<TextBanner
  type="post-login">
  post-login message
</TextBanner>
```
- ```
<TextBanner
 type="system-banner">
 system message
</TextBanner>
```

login: admin  
Password: \*\*\*\*\*

Welcome to DataPower XI52 console configuration.  
Copyright IBM Corporation 1999-2013

Version: XI52.6.0.0.0 build 231528 on 2013/06/16  
14:14:19  
Serial number: 6XXXXX

**post-login message**

**system message**

xi52#

Initial setup

© Copyright IBM Corporation 2018

Figure 2-27. Custom user interface file: CLI example

The system banner is displayed after every command submission.

The system identifier can be displayed as part of the CLI prompt: DP10:xi52#

Add the element <CustomPrompt>%s</CustomPrompt> to the user interface file.

## Auxiliary storage

- Both physical and virtual gateways support auxiliary storage:
  - XG45 (7198): Two 300-GB RAID1 drives and 300 GB usable
  - XI52 and XB62 (7199): Four 600-GB RAID10 drives and 600 GB usable
  - XG45 and XI52 virtual gateways: 16 GB (emulated RAID, resizable)
- Auxiliary storage is for storing logging data, XML files, or XSLT stylesheets
- The storage is managed as a subdirectory of the `local:` and `logstore:` directories

Figure 2-28. Auxiliary storage

After you configure and enable auxiliary data storage, you can access the available files in the defined subdirectory. This subdirectory is in the `local:` and `logstore:` directories.



## Preparing the RAID array (1 of 3)

- Administration > Storage Devices > RAID Array > raid0

Name	Status	Op-State	Logs	Administrative state
raid0	saved	up		enabled

- Initialize the array (physical gateway only):

RAID Array: raid0 [up]

Apply Cancel Undo Initialize array Synchronize array Make hot spare Perform battery-learning Delete array Activate array Initialize file system Repair file system Export View Log View Status Help

Initial setup

© Copyright IBM Corporation 2018

Figure 2-29. Preparing the RAID array (1 of 3)

RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy. The technology is used to protect data in the case of a drive failure or the deletion of a domain.

Each DataPower Gateway has a RAID array (or emulated RAID array in virtual appliances) for auxiliary storage.

Initially, `raid0` is disabled.

After you configure and enable auxiliary data storage, you can access the available files in the defined subdirectory. This subdirectory is in the `local:` and `logstore:` directories



## Preparing the RAID array (2 of 3)

RAID Array: raid0 [up]

Apply Cancel Undo Initialize array Synchronize array Make hot spare | Perform battery-learning | Delete array | Activate array Initialize file system Repair file system |

RAID Array: raid0 [up]

Apply Cancel Undo Initialize ar

Administrative state  enabled  disabled

Comments

Set to read-only  on  off

Directory

**Initialize file system**  
 (overwrites data)

Specify the **directory** that represents the array  
  
**Enable** the hard disk array

Initial setup

© Copyright IBM Corporation 2018

Figure 2-30. Preparing the RAID array (2 of 3)

Initializing the file system takes several minutes.

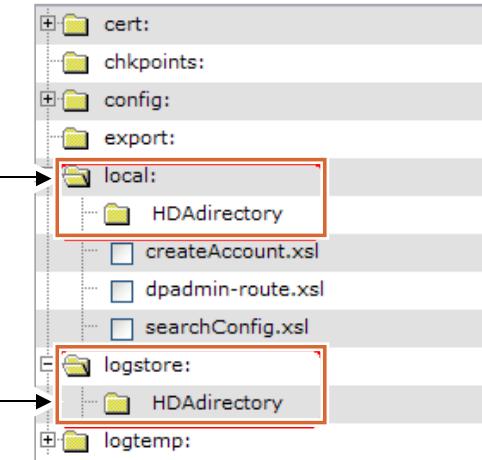
The **Directory** field is where you name the subdirectory of the `local:` and `logstore:` directories that are stored on the auxiliary storage.

The contents of the directory on the array can be marked as read-only.

## Preparing the RAID array (3 of 3)

- Other array actions for a physical disk:
  - **Activate** causes the gateway to accept a RAID array from another gateway
  - **Delete array** removes the RAID metadata from the volume
  - **Synchronize array** copies the **contents from the primary disk to** the secondary disk
  - **Make hot spare** makes a blank disk usable and synchronizes the array
  - **Repair file system** attempts to repair the RAID file system that an abnormal shutdown or other error corrupted
  - **Perform battery learning cycle** initiates a learning cycle for the RAID backup battery

A new directory is visible in each domain in **local:** and **logstore:**



Initial setup

© Copyright IBM Corporation 2018

Figure 2-31. Preparing the RAID array (3 of 3)

The RAID backup battery powers the write cache for up to 48 hours.

## Auxiliary storage on the virtual gateway

- The second virtual disk of the virtual gateway contains the auxiliary storage: 16 GB
  - Fixed size in a managed cloud environment (PureApplication System and Workload Deployer)
  - Can be changed in a stand-alone hypervisor (ESXi, and vSphere Server)
- During initial configuration under vSphere Client, you are prompted to initialize the RAID (file system)
  - If you do not initialize during the Install wizard, you can do it from a CLI command:  
`raid-volume-initialize-filesystem raid0`
- The RAID array does not need to be initialized

Initial setup

© Copyright IBM Corporation 2018

Figure 2-32. Auxiliary storage on the virtual gateway

If you increase the volume in the stand-alone hypervisor, you must reinitialize the file system to use the additional storage.

## Globalization: Displaying other languages in the Web Management service and the log

- Supported languages:
  - English
  - German
  - French
  - Italian
  - Spanish
  - Brazilian Portuguese
  - Japanese
  - Korean
  - Russian
  - Chinese: Simplified
  - Chinese: Traditional
- Language files are contained within the firmware
  - No language packs are required

Initial setup

© Copyright IBM Corporation 2018

Figure 2-33. Globalization: Displaying other languages in the Web Management service and the log

## Enabling languages

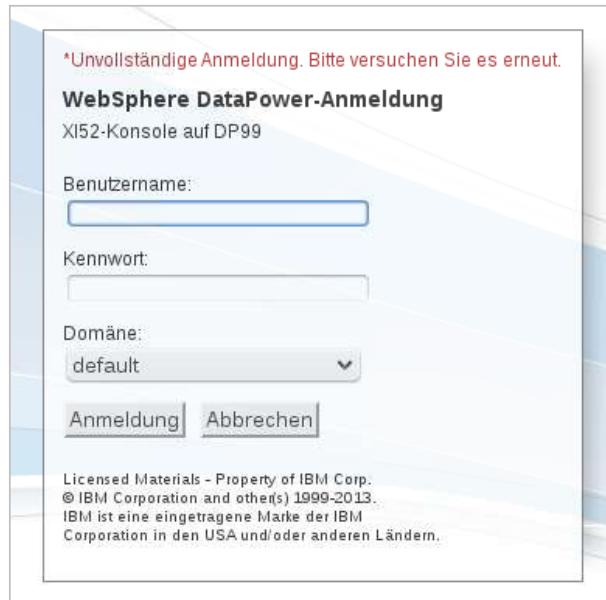
- For any language other than English, that language must be enabled before it can be used
  - If incorrect settings are made, English becomes the language
- **Administration > Device > Language**

Name	Status	Op-State	Logs	Administrative state	Comments
de	modified	up		enabled	German
en	saved	up		enabled	English
es	saved	down		disabled	Spanish
fr	saved	down		disabled	French
it	saved	down		disabled	Italian
ja	saved	down		disabled	Japanese
ko	saved	down		disabled	Korean
pt_BR	saved	down		disabled	Portuguese
ru	saved	down		disabled	Russian
zh_CN	saved	down		disabled	Simplified Chinese
zh_TW	saved	down		disabled	Traditional Chinese

Figure 2-34. Enabling languages

## Getting the WebGUI to display an alternative language

- Set the alternative language as the **primary** language in the browser
  - Location of the language option is browser-dependent
- German as the primary language in the browser:



The screenshot shows a login form titled "WebSphere DataPower-Anmeldung" for the "XI52-Konsole auf DP99". The form includes fields for "Benutzername" (username), "Kennwort" (password), and "Domäne" (domain) set to "default". Below the form is a note about incomplete registration and a copyright notice: "Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s) 1999-2013. IBM ist eine eingetragene Marke der IBM Corporation in den USA und/oder anderen Ländern."

Initial setup

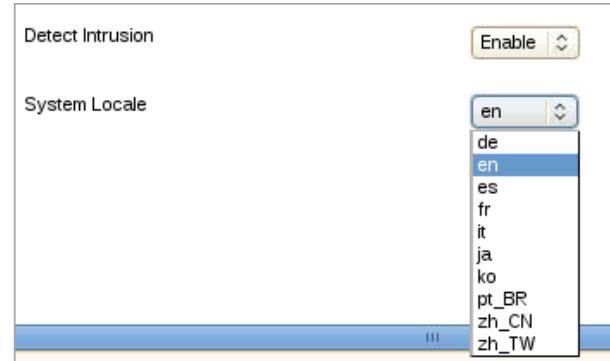
© Copyright IBM Corporation 2018

Figure 2-35. Getting the WebGUI to display an alternative language

Remember to enable the language in DataPower first.

## Getting an alternative language for the log and messages

- Administration > Device > System Settings > System Locale
- Reboot the gateway after changing the language preferences
- The alternative language must also be enabled
- Logs and messages are in the alternative language, or English if not translated



direction	client	msgid	message	Show last	<a href="#">50</a>	<a href="#">100</a>	<a href="#">all</a>
response	172.16.78.230	0x80e0039f	xmlfirewall (web-mgmt): url-open: Syntaxanalyse der Antwort aus http://127.0.0.1:63503/ abgeschlossen				
response	172.16.78.230	0x80e0039e	xmlfirewall (web-mgmt): url-open: Antwortcode 200				
request		0x80c00004	xmlfirewall (map): Von der Protokollsicht wurde kein Inhaltstyp (content-type) angegeben				
request		0x80c00004	xmlfirewall (map): Von der Protokollsicht wurde kein Inhaltstyp (content-type) angegeben				

Initial setup

© Copyright IBM Corporation 2018

Figure 2-36. Getting an alternative language for the log and messages

Set the locale for the operating language of the appliance. The locale setting manages locale-specific conventions, such as date and time formats, and controls the language of log messages. The language must be enabled before you can select it as the system locale.

## Unit summary

- Describe how to start the DataPower Gateway on the various deployment types
- Identify the Ethernet connections for physical and virtual appliances
- Use the console connector or console view for initial configuration
- Deploy a virtual appliance on various hypervisors
- Describe the minimal steps that are done during the initial configuration
- Access the Web Management graphical interface
- Configure the Ethernet interfaces for an appliance
- Configure RBM, DNS, NTP, and System Settings
- Configure user interface settings
- Prepare the appliance auxiliary storage
- Enable support for other languages for the Web Management graphical interface logs and messages

Initial setup

© Copyright IBM Corporation 2018

Figure 2-37. Unit summary

## Review questions

- 1. True or False:** The console connector/console view can be used only during the initial setup of the gateway.
- 2. In the initial setup of the gateway, which of these steps is required?**
  - A. Replace the power supplies, fans, battery, and auxiliary storage unit.
  - B. Enable the CLI over a Telnet or Secure Shell (SSH) connection.
  - C. Using the CLI, assign an IP address to an Ethernet interface and enable the Web Management service by using the enabled Ethernet interface.
  - D. Define the DNS and NTP servers.
- 3. True or False:** A domain name mismatch occurs with the default supplied certificate because the domain name where the gateway is hosted does not match the common name inside the digital certificate.

Initial setup

© Copyright IBM Corporation 2018

Figure 2-38. Review questions

Write your answers here:

- 1.
- 2.
- 3.

## Review answers

1. **False.** The console connector/console view can always be used to access the gateway. It can be available as a backup for when network communication is down.
2. **C.** In the initial setup of the gateway, which of these steps is required?
  - C. Using the CLI, assign an IP address to an Ethernet interface and enable the Web Management service by using the enabled Ethernet interface.
3. **True.** The warning displays because the domain name in the default supplied certificate does not match the domain name where the gateway is hosted.

Figure 2-39. Review answers

# Unit 3. Managing firmware

## Estimated time

00:30

## Overview

This unit shows you how to download and upgrade firmware for a DataPower appliance.

## How you will check your progress

- Review questions
- Lab exercise

## References

## Unit objectives

- Describe the actions that you can take to manage the DataPower firmware
- Download the appropriate firmware for the appliance configuration
- Describe the add-on modules for the DataPower Gateway
- Describe the tenant feature that is available for a physical DataPower Gateway
- Use the web management interface to install firmware upgrades

Figure 3-1. Unit objectives

## Actions on firmware

The actions that you can perform on firmware are:

- **Upgrade**
  - Install a firmware image that is later than the currently installed version (7.6.0.1 to 7.6.0.2)
- **Rollback**
  - Switch between the current firmware installation (primary) and the previously installed version (secondary)
- **Downgrade**
  - Install a firmware image that is earlier than the currently installed version (7.6.0.3 to 7.6.0.1)

To understand these actions, you work with the primary and secondary installations:

- **Primary** installation
  - The most current firmware image, persisted configuration, and supporting files
- **Secondary** installation
  - The previously installed firmware image, persisted configuration, and supporting files

Managing firmware

© Copyright IBM Corporation 2018

Figure 3-2. Actions on firmware

To downgrade to a previous major release (7.6.0.2 to 7.5.0.4, for example), you must reinitialize your DataPower Gateway and restore its configuration from the secure backup package that you created before you upgraded the firmware. To reinitialize, use the **reinitialize** command in **Flash** mode.

The DataPower Gateway does not migrate changes to the persisted configuration and supporting files between the primary and secondary installations.

## Release names

- Firmware images **within** a major release differ in only the last digit of the image name
  - For example, 7.5.0.1 and 7.5.0.0 are in the same major release
- Firmware images **across** major releases differ in the first 3 digits of the image name
  - For example, 7.5.0.1 and 7.2.0.2 are across major releases
- For firmware images across major releases, you must reinitialize your DataPower Gateway and restore its configuration from a secure backup package
  - Take a backup before you upgrade across major releases
  - To reinitialize, use the `reinitialize` command in Flash mode

Figure 3-3. Release names

Firmware images **within** a major release differ in only the last digit of the image name.

---

### Example

7.5.0.1 and 7.5.0.0 are in the same major release.

---

Firmware images **across** major releases differ in the first 3 digits of the image name.

---

### Example

7.2.02 and 75.0.1 are across major releases

---

For firmware images across major releases, you must reinitialize your DataPower Gateway and restore its configuration from a secure backup package.

## Restrictions for the actions on firmware

The **Upgrade**, **Rollback**, and **Downgrade** actions do not apply to:

- DataPower Gateway for Developers
- Docker platforms

These situations derive the firmware level from the source Docker image

*Figure 3-4. Restrictions for the actions on firmware*

When the platform is docker, firmware images are not installed. A Docker image that contains the DataPower Gateway version is selected with the FROM declaration in your Dockerfile.

## Requirements to perform an upgrade

The following steps assume:

- You have the appropriate administrative access:
  - For web management access, administrative access in the **default** domain
  - For CLI access, you need administrative access to the **flash** mode
- You have an IBM Support account to download new firmware images from IBM Fix Central
- You have the appropriate authority to access previously downloaded and stored firmware images on your remote file or web server
- During firmware maintenance, the appliance is “offline”:
  - The running configuration is persisted as the startup configuration
  - The appliance is quiesced (not accepting new requests)
  - The appliance is not actively processing messages (quiesce is complete)
  - You are the only active user that is logged on to the appliance

Figure 3-5. Requirements to perform an upgrade

Ensure that you have the appropriate administrative access to the default domain on the appliance, and that you can access the downloaded firmware images on your remote file or web server.

Also ensure that the appliance is quiesced before upgrading the appliance.

## Suggested procedure for upgrading

1. Identify features with feature-specific libraries
  2. Determine the firmware image to download
  3. Download the firmware image from IBM Fix Central
  4. Back up the current gateway configuration
  5. Optional: Restart the gateway
  6. Transfer the downloaded firmware image
  7. Install the firmware image
  8. Verify the new firmware version
- 
- Additional upgrade information from IBM Support:
    - Knowledge Collection: How to upgrade the firmware on an IBM DataPower Gateway Appliance  
<http://www.ibm.com/support/docview.wss?uid=swg27015333>

Figure 3-6. Suggested procedure for upgrading

For more information on how to upgrade, refer to the article  
<http://www.ibm.com/support/docview.wss?uid=swg27015333>

## Step 1. Identify features with feature-specific libraries

- Identify the supported libraries in the running firmware
  - Different versions of the firmware for different libraries
- Retrieve the installed features and libraries from the current firmware
  - Web management: **Device Features and Library Information**
  - CLI: **show features** and **show library**

Features that require feature-specific libraries		
Name in web management	Name in CLI	Value in firmware image name
Extended Oracle support for the Database Connectivity Option	DCO-Oracle	oradco
TIBCO EMS	Tibco EMS	tibco

- This step does not apply if the platform is **Docker**

Figure 3-7. Step 1. Identify features with feature-specific libraries

Some of the add-on features require that a feature-specific library be included in the downloaded firmware.

## Step 2. Determine the firmware image to download

Fix Central contains firmware for different combinations of appliance models, firmware versions, libraries, and features.

Firmware file naming structure: ***productVRMF.licenses.scryptn***

- ***product***: Relates to the machine type: *idg* is for a non-Docker non-Linux IBM DataPower Gateway, *idg\_dk* is when the platform is docker, *idg\_linux* is when the platform is Linux, *xg* is XG45, *xi* is XI52, and *xb* is for XB62
- ***VRMF***: The specific firmware version (7603 is V7.6.0.3)
- ***licenses***: Which other licenses are supported that are not included in the base firmware: oradco, tibco, tenant
- ***scryptn***: The firmware format:
  - *scrypt3* is for IDG, XG45, XI52, and XB62 physical gateways
  - *scrypt4* is for IDG virtual gateways (none for XG45, XI52, XB62)

*idg7603.scrypt4*

- A V7.6.0.3 image that works on a virtual IBM DataPower Gateway
- Includes support for the following features:
  - SQL: SQL-ODBC or Database Connectivity Option (installed only if licensed)
  - Security Access Manager, all versions (installed only if licensed)
  - IBM MQ / WebSphere JMS

Managing firmware

© Copyright IBM Corporation 2018

Figure 3-8. Step 2. Determine the firmware image to download

VRMF is version, release, modification, fix.

“Tenant” is a version of firmware that allows partitioning of memory and CPU on a physical gateway.

Unless you are an IBM Business Partner who requires Application Specific Licensing (ASL) images, do not download packages from IBM Fix Central that state “For ASL Partners”.

### Step 3. Download the firmware image from Fix Central

- **[www.ibm.com/support/fixcentral](http://www.ibm.com/support/fixcentral)**
- Search for the product: IBM DataPower Gateways
- Download options are: Browser (HTTPS), Download Director (requires Java), or bulk FTPS
- Must have an IBM Universal ID

The screenshot shows the IBM Fix Central interface. On the left, there is a list of fix packs:

- 1 fix pack: → IDG-virtual-7.6.0.3-Firmware**  
DataPower-7.6.0.3-IDG-virtual  
[Fix list](#)
- 2 fix pack: → IDG-8436-7.6.0.3-Firmware**  
DataPower-7.6.0.3-IDG-8436  
[Fix list](#)
- 3 fix pack: → XG45-2426-7198-7.6.0.3-Firmware**  
DataPower-7.6.0.3-XG45-2426-7198  
[Fix list](#)

A yellow arrow points from the link for fix pack 1 to the right panel. The right panel displays the contents of the selected fix pack:

**fix pack: IDG-virtual-7.6.0.3-Firmware**

<a href="#"> idg7603.scrypt4</a>	(663.98 MB)
<a href="#"> idg7603.tibco.scrypt4</a>	(664.83 MB)
<a href="#"> idg7603.oradco.scrypt4</a>	(670.02 MB)
<a href="#"> idg7603.tibco.oradco.scrypt4</a>	(670.88 MB)
<a href="#"> idg_linux.7603.scrypt4</a>	(726.41 MB)
<a href="#"> idg_linux.7603.tibco.scrypt4</a>	(727.21 MB)
<a href="#"> idg_linux.7603.oradco.scrypt4</a>	(732.47 MB)
<a href="#"> idg_linux.7603.tibco.oradco.scrypt4</a>	(733.26 MB)
<a href="#"> idg_docker7603.tar.gz</a>	(238.33 MB)
<a href="#"> aoc-war-7603.tar</a>	(130 KB)

© Copyright IBM Corporation 2018

Figure 3-9. Step 3. Download the firmware image from Fix Central

This example is for an virtual IBM DataPower Gateway for Version 7.6.0.3.

The tar.gz file is the Docker image at V7.6.0.3

The aoc-war-7603.tar file contains the ODCINFO web application for the option for application optimization feature.

## Step 4. Back up the current gateway configuration

- Depending on business requirements, you might want to back up the configurations on the gateway **before** the upgrade
- Easiest to back up all domains at once from the **default** domain
  - Use the Export utility or the secure backup approach
- To export:
  - Web management: **Export Configuration**
  - CLI: **backup** command
- To secure backup:
  - Web management: **Secure Backup** under **System Control**
  - CLI: **secure-backup** command
- After export or secure backup, copy the backup file from the gateway to a secure file store
- Cannot use secure restore after the upgrade because of the firmware level changes between the backup and the restore actions
  - Secure backup / secure restore is not supported for Docker platforms

Figure 3-10. Step 4. Back up the current gateway configuration

Ensure that you take a backup before you upgrade across major releases.

You are required to reinitialize the appliance and then you must restore your configuration on the new version.

## Step 5. Optional: Restart the gateway

- Rebooting the appliance before a firmware upgrade clears the memory and the temporary file space
  - Was a common practice for a previous DataPower series
  - Not common for the newer series (IDG, XG45, XI52, and XB62)
- Might be necessary if upgrading a V6 virtual appliance to V7 firmware
  - The V7 firmware size approaches the limit of the temporary storage, which is needed for firmware upgrade activities

*Figure 3-11. Step 5. Optional: Restart the gateway*

Restarting the gateway is recommended to clear memory and temporary space when you are upgrading from a much earlier version of the DataPower gateway.

## Step 6. Transfer the downloaded firmware image

- The firmware must be copied into the **image:** directory
- Web management: The firmware file can be uploaded from a workstation or fetched from a server: **Boot Image** section of **System Control**



- CLI: The firmware can be loaded only from a remote service by using HTTP, HTTPS, SCP, or SFTP by using the **copy** command

Figure 3-12. Step 6. Transfer the downloaded firmware image

The firmware file can be uploaded from a workstation or fetched from a server: **Boot Image** section of **System Control** in the WebGUI or Blueprint Console.

## Step 7. Install the firmware image

- Specify the new firmware from the **image:** directory and reboot the gateway
- Web management: **Boot image** section of **System Control**

The screenshot shows a user interface for booting a new firmware image. At the top, there's a checkbox labeled "I accept the terms of the license agreements." followed by a checked checkbox icon. Below it is a dropdown menu labeled "Firmware File" with the value "idg7603.script4". To the right of the dropdown are two buttons: "Upload..." and "Get". At the bottom of the form is a large orange-bordered button labeled "Boot Image".

- CLI: **boot image** command
- The appliance validates the encrypted and signed firmware image, and then boots into the new firmware image
  - The reboot operation takes several minutes. If the new firmware contains an update to any of the base components of the firmware, it could take up to 20 minutes
- When the platform is **Docker**, firmware images are not installed. A Docker image that contains the wanted firmware version is selected with the **FROM** declaration in your Dockerfile.

Managing firmware

© Copyright IBM Corporation 2018

*Figure 3-13. Step 7. Install the firmware image*

The “boot image” command has a parameter for the “accept license” argument, and a parameter for the Image file name.

## Step 8. Verify the upgrade operation

- After the appliance reboots, verify that it is running the firmware version that you want
- Web management: Check the firmware that is listed under **About** choice for the **Help** icon, or under **Version Information**

Version Information	
Serial	0000000
Version	IDG.7.6.0.3
Build	292006
Build date	Sep 29, 2017 9:43:50 AM
Watchdog build	IDG.7.6.0.3
Installed DPOS	IDG.7.6.0.3
Running DPOS	IDG.7.6.0.3
XML accelerator	Embedded
Machine type	5725
Model type	T09
Tenant name	

- CLI: **show firmware-version** command

Figure 3-14. Step 8. Verify the upgrade operation

After the appliance reboots, verify that it is running the firmware version that you want.

## Roll back the firmware

- The gateway retains a copy of the previous firmware in its file system
  - If the current firmware causes problems, you can easily revert to a previous firmware image
- Only a single rollback is possible
  - Cannot roll back to multiple, previous firmware images
  - Secondary installation becomes the primary installation
  - Further rollbacks switch between the primary and secondary installation
- Web management: **Switch Installation Image** section in **System Control**



- CLI: Use the **boot switch** command to roll back to a previous firmware image

Figure 3-15. Roll back the firmware

Make sure that you save the appliance configuration before you roll back the firmware because the appliance reboots and any unsaved changes are lost.

The **boot delete** CLI command can be used to delete the secondary image.

## Add-on module and feature management

- Add-on modules are a packaging of specific features
    - Modules are purchased from IBM Passport Advantage
    - Received package contains an activation tool and installation instructions
      - Activation tool is “loaded” with a **boot image**
      - Feature is enabled after restart
    - After activation, features can be disabled and re-enabled
      - Disable/enable tools are on IBM Fix Central
      - Search on the text “tools”
      - Disable/enable tools are loaded with a **boot image**
    - You cannot activate modules on DataPower Gateway for Developers. To activate modules, you **must** convert DataPower Gateway for Developers to DataPower Gateway Virtual Edition.
- The conversion tool is available from IBM Passport Advantage.

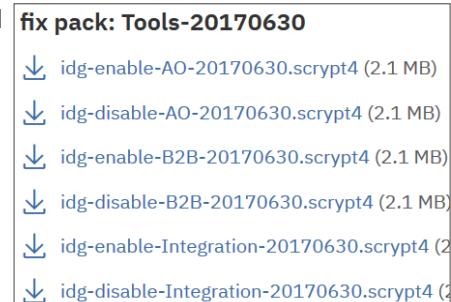


Figure 3-16. Add-on module and feature management

Many add-on modules are included by default in the IBM DataPower Gateway.

For a complete list of available modules by product, see

[https://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0/com.ibm.dp.doc/feature\\_available.html](https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/feature_available.html)

## Product packaging: optional modules

- Integration module
  - Binary processing, SQL, IMS integration
- B2B module
  - Binary processing, SQL, B2B transaction processing, and protocol
- IBM Security Access Manager (ISAM) Proxy module
  - Interaction with IBM Security Access Manager (ISAM) for Web policy enforcement via a reverse proxy service
- Application Optimization (AO) module
  - Self-balancing of clustered appliances, intelligent load distribution across back-end application servers, On-Demand Router support to WebSphere servers
- Tenant module
  - Supports multiple firmware images running on a physical gateway
- TIBCO EMS module
  - Message interaction with TIBCO Enterprise Management Service (EMS)
- Database Connectivity module
  - Database connectivity with support for complex Oracle data types and extended Oracle support
- Data Integration module
  - Specifically for the XG45, Binary processing, SQL

*Modules can be ordered at initial purchase or after installation*

Figure 3-17. Product packaging: optional modules

This slide lists the optional modules that are available in Version 7.6.0.

- Integration module – This supports binary processing, SQL, and IMS integration.
- B2B module – This module supports binary processing and SQL similar to the Integration module, but it also adds B2B transaction processing and protocols.
- ISAM Proxy module – This module supports interaction with IBM Security Access Manager (ISAM) for Web policy enforcement via a reverse proxy service.
- Application Optimization (AO) module – This module provides for self-balancing of clustered appliances, intelligent load distribution across back-end application servers, and On-Demand Router support for WebSphere servers.
- Tenant module – This module supports multiple firmware images to run concurrently on the same physical IBM DataPower Gateway.
- TIBCO EMS module – This module allows message interaction with TIBCO Enterprise Management Service.
- Database Connectivity module – This module supports database connectivity with support for complex Oracle data types and extended Oracle support.
- Data Integration module – This module is specifically for the XG45 model, and adds binary processing and SQL.

A key point is that the modules can be ordered at initial purchase, or after the initial install of the appliance.

## Product packaging: physical gateway optional modules

Module	IDG	XG45	XI52	XB62
Integration <sup>1</sup>	Yes	No	Built-in	Built-in
B2B <sup>1</sup>	Yes	Yes	Yes	Built-in
ISAM proxy	Yes	Yes	Yes	Yes
AO	Yes	Yes	Yes	Yes
Tenant	Yes	No	No	No
TIBCO EMS	Yes	No	Yes	Yes
Data Connectivity <sup>1</sup>	No	No	Yes	No
Data integration <sup>1</sup>	No	Yes	No	No

<sup>1</sup> This module includes the “extended Oracle support for the Database Connectivity feature”, which is separately managed

Figure 3-18. Product packaging: physical gateway optional modules

This table documents the available modules and which physical gateways support them.

Although this webcast focuses on the IBM DataPower Gateway, or IDG, the older gateways are shown so that you can see that the different models have different capabilities. The newer IDG simplified this by being the only model in the 9006 series, but with the different capabilities available through the optional modules.

The IBM DataPower Gateway supports all of the modules, except for the Data Integration module. Remember that the Data Integration module was for the XG45 only. More importantly, Data Integration module capabilities are already available in the new Integration module. IDG is the only physical gateway that supports the Tenant module.

The XG45 model supports most of the modules. The Integration module is not supported, but the Data Integration module is. The only capability between the two modules that remains unavailable is IMS connectivity. The TIBCO EMS module is also not available.

The XI52 already supports the capabilities of the Integration module. The Data Integration module and Data Connectivity module are not available because the built-in support already covers those capabilities. The remaining modules are available.

The XB62 has the Integration and B2B modules already built-in. The Data Integration module and Data Connectivity module are not available because the built-in support already covers those capabilities. The remaining modules are available.

## Product packaging: virtual gateway optional modules

Module	developers edition	nonproduction edition	production	for developers
Integration <sup>1</sup>	Activated	Activated	Yes	Activated
B2B <sup>1</sup>	Activated	Activated	Yes	Activated
ISAM proxy	Activated	Yes	Yes	No
AO	Activated	Activated	Yes	Activated
Tenant	No	No	No	No
TIBCO EMS	No	Yes	Yes	No
Data Connectivity <sup>1</sup>	No	No	No	No
Data integration <sup>1</sup>	No	No	No	No

<sup>1</sup>This module includes the “extended Oracle support for the Database Connectivity

Managing firmware

feature”, which is separately managed

© Copyright IBM Corporation 2018

Figure 3-19. Product packaging: virtual gateway optional modules

For **all** of the virtual editions, the Data Integration, Data Connectivity, and Tenant modules are not available because the capabilities are already part of the Integration module, or require a physical gateway.

The Developers edition does NOT support the TIBCO EMS module. The remaining modules are available, and the licenses are already activated.

The Nonproduction edition supports most of the modules. The ISAM proxy and TIBCO EMS modules require a license to activate the support.

The Production edition also supports most of the modules. All of the available modules require a license to be activated.

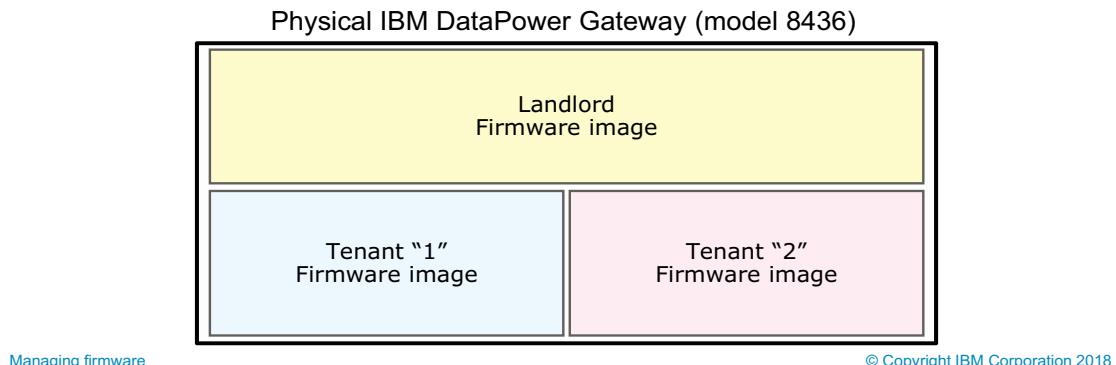
The ISAM Proxy module is not available for the developers edition, nonproduction edition, and the production edition when the platform is **docker**.

For a complete list of available modules by product, see

[https://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0/com.ibm.dp.doc/feature\\_available.html](https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/feature_available.html)

## Tenant feature (1 of 5)

- The Tenant feature supports running multiple firmware “images” on the same gateway
  - Supported on a physical IBM DataPower Gateway (model 8436) only
- Provides runtime isolation and firmware upgrade flexibility for IBM API Connect and traditional DataPower workloads
- The feature supports a “primary” firmware image (the “landlord”), and up to two “subsidiary” firmware images (the “tenants”)



*Figure 3-20. Tenant feature (1 of 5)*

The tenant module supports the creation of 2 API Connect tenants and the installation of their initial firmware image.

Since tenants use a different firmware image, you must download tenant-specific firmware images from IBM Fix Central to manage the firmware version on tenants.



## Tenant feature (2 of 5)

- Besides the physical gateway requirement, the Tenant feature also requires:
  - An activated Tenant Module that is obtained from IBM Passport Advantage
  - A tenant-specific firmware image from IBM Fix Central

[idg7603.tenant.scrypt3 \(801.4 MB\)](#)

- A tenant is installed from the **default** domain of the landlord image
  - Name the tenant
  - Specify an image name

The screenshot shows the 'Install Tenant Firmware' dialog box. It includes the following fields and controls:

- I accept the terms of the license agreements.:**
- Name of the Tenant Gateway:**
- Tenant Firmware File:**
- Buttons:** Upload..., Fetch..., Edit..., View...
- Install Tenant Firmware**

Managing firmware

© Copyright IBM Corporation 2018

Figure 3-21. Tenant feature (2 of 5)

A tenant is installed from the **default** domain of the landlord image.

## Tenant feature (3 of 5)

- The **Tenant** object in the landlord identifies the configured tenant images

The screenshot shows a management interface for configuring tenants. On the left, a table lists two tenants: tenant01 (Status: saved, Op-State: down, Comments: disabled) and tenant02 (Status: modified, Op-State: up, Comments: enabled). On the right, detailed configuration settings are shown for tenant02:

CPU threads:	38
Memory:	8
Telnet service name:	telnet1
Telnet address:	9.37.130.152
Telnet port:	2300
SSH address:	9.37.130.152
SSH port:	2301
Web management address:	9.37.130.152
Web management port:	9998

**Install Tenant Firmware**

Managing firmware © Copyright IBM Corporation 2018

Figure 3-22. Tenant feature (3 of 5)

The port specifications for the management services in the tenant can also be specified in the tenant itself.

## Tenant feature (4 of 5)

- The tenants inherit the following settings from the landlord:
  - Network interfaces and settings
  - Time and date (but time zone is customizable)
  - NTP service
- The tenant inherits its activated features from the landlord, except for (these features cannot be licensed on the tenant):
  - Access Manager Proxy feature
  - Self-balancing feature of the AO module
  - B2B module
  - IBM IMS feature
  - TIBCO EMS feature
- The feature licensing is inherited from the landlord
  - Tenants cannot license additional features
  - Tenants cannot access certain features on the landlord such as RAID

Figure 3-23. Tenant feature (4 of 5)

Tenants cannot access these resources on the gateway:

- RAID storage
- Intelligent Platform Management Interface (IPMI)
- Hardware Security Module (HSM)

## Tenant feature (5 of 5)

- From the **default** domain of the landlord, you can delete a tenant
- You can reinitialize (“factory reset”) the **landlord**, but the tenant images and connection details are lost
  - Can use a secure backup to preserve the tenant state for later secure restore
- You can reinitialize (“factory reset”) the **tenant**, and the firmware and state is deleted
  - Tenant connection details are in the landlord, so they must be explicitly deleted
- When the landlord is restarted or stopped, the tenant network connections are unavailable until the landlord is operational
  - When a tenant is restarted or stopped, it affects only its own network connections

Figure 3-24. Tenant feature (5 of 5)

You can reinitialize (“factory reset”) the **landlord**, but the tenant images and connection details are lost.

Use a secure backup to preserve the tenant state for later secure restore.

## Unit summary

- Describe the actions that you can take to manage the DataPower firmware
- Download the appropriate firmware for the appliance configuration
- Describe the add-on modules for the DataPower Gateway
- Describe the tenant feature that is available for a physical DataPower Gateway
- Use the web management interface to install firmware upgrades

Figure 3-25. Unit summary

## Review questions

1. Which of the following file extensions is appropriate for a virtual appliance?
  - A. scrypt2
  - B. scrypt3
  - C. scrypt4
  - D. scryptv
2. **True or False.** The firmware image that is running on an appliance can be upgraded directly from an external HTTP server.
3. **True or False.** Each administrator must register for an IBM ID before access to the DataPower download site is granted.

Figure 3-26. Review questions

Write your answers here:

- 1.
- 2.

## Review answers

1. **C.** Which of the following file extensions is appropriate for a virtual appliance?
  - A. scrypt2
  - B. scrypt3
  - C. scrypt4**
  - D. scryptv
2. **False.** Firmware images must be uploaded to the appliance **image:/// directory** before upgrading the firmware.
3. **True.** Each administrator must register for an IBM ID before access to the DataPower download site is granted.

Figure 3-27. Review answers

## Exercise 1

- Upgrading image firmware

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

5.0

Figure 3-28. Exercise 1

## Exercise objectives

After completing this exercise, you should be able to:

- Identify the current firmware level on the gateway
- Upgrade the firmware level on the gateway
- Switch the installation image between the current and the previous version of the firmware.

*Figure 3-29. Exercise objectives*

---

# Unit 4. DataPower administration overview

## Estimated time

01:15

## Overview

This unit shows you how to manage the DataPower appliance by using the various management interfaces, such as the CLI, SOAP, and the WebGUI. You learn how to manage resources on the DataPower flash memory. You also learn good practices for securing the DataPower appliance.

## How you will check your progress

- Review questions

## References

IBM DataPower Gateways 7.6.0 product documentation:

[http://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0](http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0)

## Unit objectives

- List the methods that can be used to administer the DataPower appliance
- Work with files on the DataPower appliance
- Determine the status of various aspects of the appliance
- Run secure backup and restore
- Quiesce traffic to the appliance

Figure 4-1. Unit objectives

## DataPower Appliance administration

- Perform administration tasks on the DataPower gateway by using one of the following interfaces:
  - Command-line interface (CLI)
    - Connect with serial connection, SSH, or Telnet (Telnet not recommended)
  - Web access
    - WebGUI (traditional web interface)
    - Blueprint Console (updated web interface)
  - XML management API
    - SOAP requests
  - REST management API
    - REST requests



DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-2. DataPower Appliance administration

Only the console connection is active for use when the gateway is first installed. The administrator must enable the other three administration interfaces by using the command-line interface.

The console connector on the front panel of the IDG is an RJ45 connector. Two cables are supplied with the gateway: an RJ45-to-DB9 cable, and an RJ45-to-USB cable. A virtual gateway uses the serial console facility of the platform to provide the original CLI connection.

You can enable the web management server, a CLI over Telnet or Secure Shell (SSH), or the XML management web service over **one** of the Ethernet interfaces, or **all** Ethernet interfaces. Typically, the administration services are only available over an internal network connection while external traffic flows through the remaining Ethernet interfaces. The XML management API is a web service that accepts administration commands. The web service can also accept WS-Management and SNMP management commands.



## Web management interface

- Administrators use the web management interface to configure and troubleshoot the DataPower gateway
  - The web management interface must be activated through the command-line interface before its first use
  - Role-based management restricts access to predefined administrators and those individuals who perform configuration
  - The web management interface is also used by developers to create and edit application services
- Using a web browser, type the network address and the port that is assigned to the web management interface
  - The default port for the WebGUI application is 9090
  - Always use HTTPS



DataPower administration overview

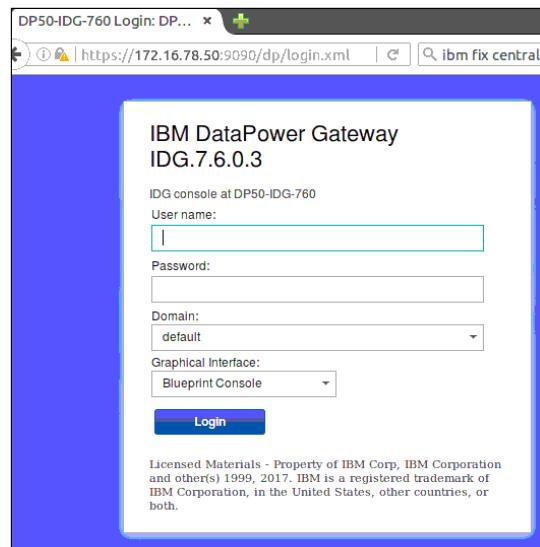
© Copyright IBM Corporation 2018

Figure 4-3. Web management interface

Remember to enter the `https` protocol in front of the network host name or address for your DataPower gateway. The default value that is provided in the documentation is port 9090 for the web management interface. However, you are free to assign any port number in range for this administration interface.

## Web management login page

- The login page
- Notice that the URL is redirected
  - Suffix by **/dp/login.xml**
- Enter:
  - User name
  - Password
  - Domain
  - Graphical Interface
    - WebGUI
    - Blueprint Console (default)



DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-4. Web management login page

The URL redirects to the Blueprint Console login URL. You can still request the WebGUI interface on this page.

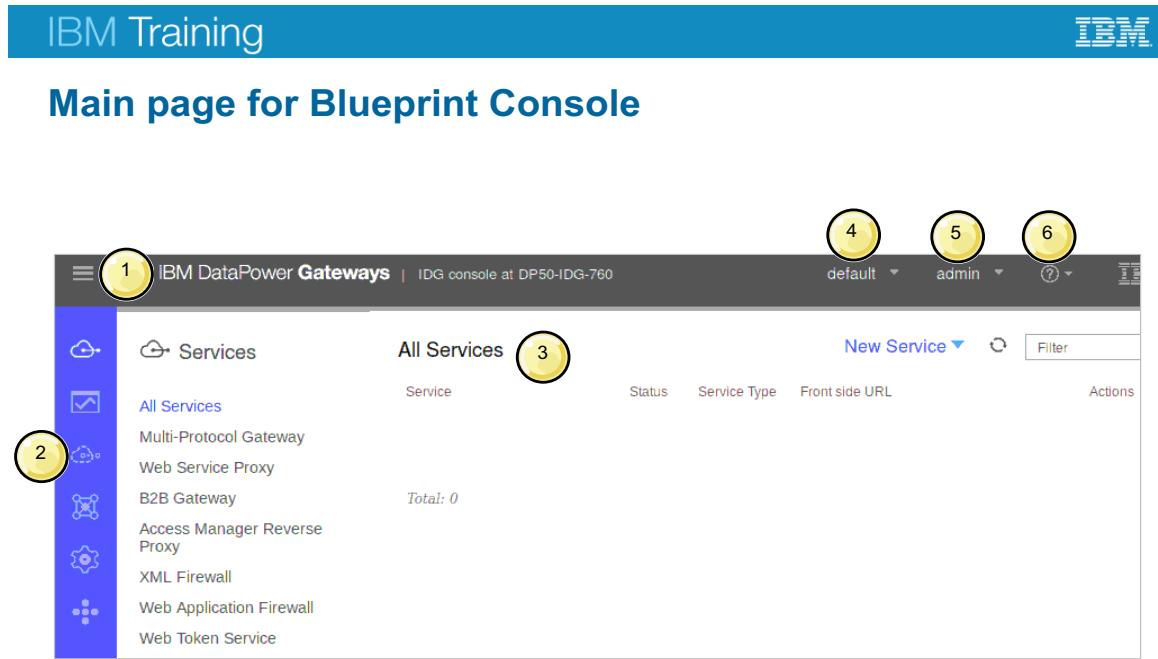


Figure 4-5. Main page for Blueprint Console

1. The Menu icon (“hamburger” icon) provides a specialized selection list.
2. The navigation bar provides access to configuration or management options.
3. The **All Services** pane lists all of the services, regardless of type, that are configured in this domain. For the example, which shows the default domain, no services are configured.
4. This menu choice displays the current domain that the user is accessing, and the drop-down lists the other selectable domains.
5. This menu choice displays the logged-in user name. The drop-down list contains the “logout” selection.
6. The Help icon (circled question mark) lists:
  - a. The About information on the firmware version
  - b. A link to the IBM Knowledge Center
  - c. A link to the IBM Support Portal
  - d. A link to generate an Error Report
  - e. An option to open the WebGUI

The screenshot shows the main interface of the IBM WebSphere DataPower XI52 WebGUI. The top navigation bar includes the title 'WebSphere, DataPower XI52', the user 'admin @ DP99', and the IBM logo. The left sidebar has a 'Control Panel' icon with a yellow circle containing the number 1, and a 'Pattern Console' icon. Below these are links for Status, Services, Network, Administration, and Objects. A message at the top right says 'Intensive Level of Logging is enabled, which impacts performance. Change Troubleshooting settings.' The main content area is divided into four sections: 'Services' (with icons for Web Service Proxy, Multi-Protocol Gateway, XML Firewall, Web Application Firewall, and XSL Accelerator), 'Monitoring and Troubleshooting' (with icons for View Logs, Troubleshooting, Web Services Monitor, and View Status), and 'Files and Administration' (with icons for File Management, System Control, Import Configuration, Export Configuration, and Keys & Certs Management). The bottom of the page includes copyright information: 'Firmware: XI52.8.0.0.0 Build: 231528 IBM WebSphere DataPower Copyright IBM Corporation 1999-2013 View License Agreement' and 'DataPower administration overview © Copyright IBM Corporation 2018'.

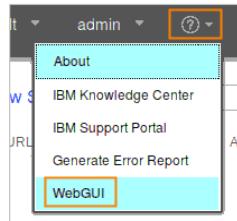
Figure 4-6. Main page for WebGUI

1. The navigation bar provides access to configuration or management options. The Control Panel icon and the Pattern Controls icon allow you to switch between displays.
2. The control panel provides quick access to common administration functions. The Services section allows you to create or modify the primary DataPower services.
3. The Monitoring and troubleshooting section provides a view of the DataPower Appliance status, traffic, and load.
4. The Files and Administration section manages the configuration files, access levels, and cryptographic keys and certificates on the gateway.

All links on the Control Panel are also available through the navigation bar.

## Switching between Blueprint Console and WebGUI

- The Blueprint Console and WebGUI run as separate tabs in the browser
- To get to the WebGUI from the Blueprint Console:
  - Help icon > WebGUI



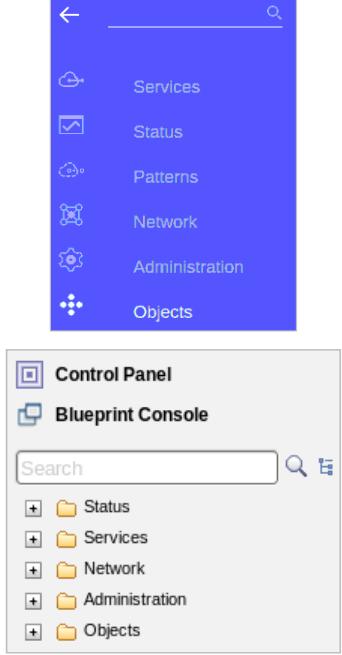
- To get to the Blueprint Console from the WebGUI:
  - Blueprint Console in navigation bar



DataPower administration overview

© Copyright IBM Corporation 2018

*Figure 4-7. Switching between Blueprint Console and WebGUI*



The screenshot shows the IBM DataPower administration interface. At the top left is the "IBM Training" logo. At the top right is the "IBM" logo. Below the header is a section titled "Navigation bar categories". To the left of the table is a sidebar with icons and labels: Services, Status, Patterns, Network, Administration, and Objects. Below this is a "Control Panel" section with "Blueprint Console" and a search bar. A tree view shows "Status", "Services", "Network", "Administration", and "Objects".

Category	Description
Services	Configure services that accelerate, secure, and integrate XML-based applications
Status	Provides access to real-time operational data maintained by the gateway's management system
Patterns	Configure service patterns that act as templates to create similar services. Available in Blueprint Console only
Network	Configure network services and interfaces and retrieve information about network connectivity
<b>Administration</b>	Provides access to troubleshooting, logging, access control, and file and configuration administration
Objects	Provides direct access to the <i>object store</i> that represents the configuration for the entire gateway

DataPower administration overview © Copyright IBM Corporation 2018

Figure 4-8. Navigation bar categories

The following three pages focus on the administration features found in the Blueprint administration console.



## System control features (1 of 3)

The screenshot shows the 'System Control' page. On the left, a navigation bar has a 'System Control' link highlighted with a yellow circle labeled '1'. The main content area has five numbered callouts:

- 2**: 'Set Time and Date' section. It says 'Time and Date cannot be configured while NTP Service is in use.' with a note about editing NTP service settings.
- 3**: 'Boot Image' section. It includes a checkbox for accepting license terms and a dropdown for selecting a firmware file, with buttons for Upload..., Fetch..., Edit..., and View.
- 4**: 'Switch Installation Image' section. It has a button for 'Switch Installation Image'.
- 5**: 'Select Configuration' section. It includes a dropdown for 'Configuration File' (set to '(none)'), with buttons for Upload..., Fetch..., Edit..., and Select Configuration.

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-9. System control features (1 of 3)

The **System Control** page groups several system-wide updates that affect the firmware, clock, and system certificate. Certain options are only available from the default domain.

1. Access the System Control page through the Administration section of the navigation bar.
2. Use the time and date features to set the current time in your locale. To modify the time zone, click **Administration > Device > Time Settings** from the navigation bar. This screen capture shows a gateway where the time and date are controlled from an NTP service. The NTP service to use is set in **Network > Interface > NTP Service**.
3. Use the **Boot Image** feature to upgrade the system to a newer firmware level. Use the **Upload** function to copy a new firmware image onto the DataPower gateway. When this process is complete, click **Boot Image** to restart the DataPower gateway with the new firmware.
4. If you encounter problems when you use a new firmware level, click **Switch Installation Image** to revert the DataPower gateway to the previous firmware level.
5. The **Select Configuration** section determines which configuration file is used on the next system restart. Without a configuration, the DataPower gateway uses the **config:///autoconfig.cfg** file. The configuration file must be in the **config:** directory.



## System control features (2 of 3)

The screenshot shows the 'System Control' interface with four main sections highlighted by yellow circles and numbered 1 through 4:

- 1. Secure Backup:** Allows creating a backup of the gateway configuration. Fields include 'Crypto certificate' (dropdown), 'Destination' (text input), and 'Include RAID' (radio buttons). A 'Secure Backup' button is present.
- 2. Secure Restore:** Imports a secure backup copy onto a gateway. Fields include 'Crypto credentials' (dropdown), 'Source' (text input), and 'Only validate the backup' (radio buttons). A 'Secure Restore' button is present.
- 3. Shutdown:** Reinitializes the gateway. Fields include 'Mode' (dropdown set to 'Reboot system'), 'Delay' (text input set to '10'), and a 'Shutdown' button.
- 4. Change User Password:** Changes the user password. Fields include 'Old Password' (text input), 'New Password' (text input), 'Confirm Password' (text input), and a 'Change User Password' button.

On the left side of the interface, there are three buttons with arrows pointing to them:

- Power off system**
- Reboot system**
- Reload firmware**

At the bottom of the page, the footer reads 'DataPower administration overview' on the left and '© Copyright IBM Corporation 2018' on the right.

Figure 4-10. System control features (2 of 3)

This page continues examining the System Control page.

1. **Secure Backup** creates a backup of the gateway configuration. What differs from a standard backup is that a secure backup contains private keys and certificates. The secure backup can optionally contain the data in the auxiliary storage or any iSCSI device. A certificate must be specified to use the encryption of the secure backup copy. The destination for this file is specified as well. An unencrypted XML manifest file is produced, listing the date of the backup, firmware level, and serial number of the backed-up gateway. The gateway must be initialized with the secure backup mode enabled for secure backup to be possible.
2. **Secure Restore** imports a secure backup copy onto a gateway, completely replacing the original contents (not a merge). The location of the secure backup file and the crypto certificate that is used to encrypt it must be specified. The gateway that imports the secure backup must be at the same firmware level, and have a compatible configuration (auxiliary storage and features, for example). The validate option processes the secure backup file, but does not write anything to the gateway. The gateway must be initialized with the secure backup mode enabled for secure restore to be possible.
3. Use the **Shutdown** option to reinitialize the DataPower gateway in one of three modes:

- **Power off system** stops the DataPower gateway and turns off the power. For cloud platforms and Docker, you cannot use this command to turn off the power to the host system.
  - **Reboot system** restarts the DataPower gateway. All temporary files and unsaved configuration changes are lost.
  - **Reload firmware** restarts the device without rebooting the gateway. Temporary files are not lost, and unsaved changes are kept intact.
  - **Halt system** stops the gateway but power remains on. This keyword is deprecated. Use **power off** instead.
4. Use the **Change User Password** section to assign a new password to the currently logged in user. If you are logged in as admin, this operation changes both the web management and CLI passwords for the user.

The screenshot shows the 'System control features (3 of 3)' section of the IBM DataPower administration interface. It lists five numbered steps:

- 1** Restart Domain (button)
- 2** Reset Domain (button)
- 3** Generate Device Certificate (deprecated) (button)
  - Common Name (CN) input field
  - Generate Self-Signed Certificate  on  off \* button
  - Generate Device Certificate (deprecated) button
- 4** Quiesce (button)
  - Timeout input field seconds \*
  - Delay input field 0 seconds
  - Quiesce button
- 5** Unquiesce (button)

Figure 4-11. System control features (3 of 3)

This page continues examining the System Control page.

1. **Restart Domain** reloads the configuration for the current application domain. Any unsaved configuration changes are lost.
2. **Reset Domain** deletes the configured objects within the domain, but retains the files in the local: directory. The domain continues to exist.
3. **Generate Device Certificate** creates a digital certificate, which represents the current DataPower gateway. The common name must be mapped to a valid IP host address. This option is now deprecated. Use the Crypto Tools key generation to create a private key and public certificate for the gateway.
4. **Quiesce** blocks new transactions to the gateway, while allowing existing transactions complete. This operation changes protocol handlers to the down operational state, changes services to the down operational state, and changes domains to the down operational state. When the default domain is quiesced, it does not change to the down operational state. Quiescing proceeds in a child-parent relationship, where protocol handlers are quiesced first, then the services, and then the domains.
5. **Unquiesce** allows the gateway to process transactions. Objects that were previously quiesced are now changed into the up state. Making these transitions proceeds in the reverse order as

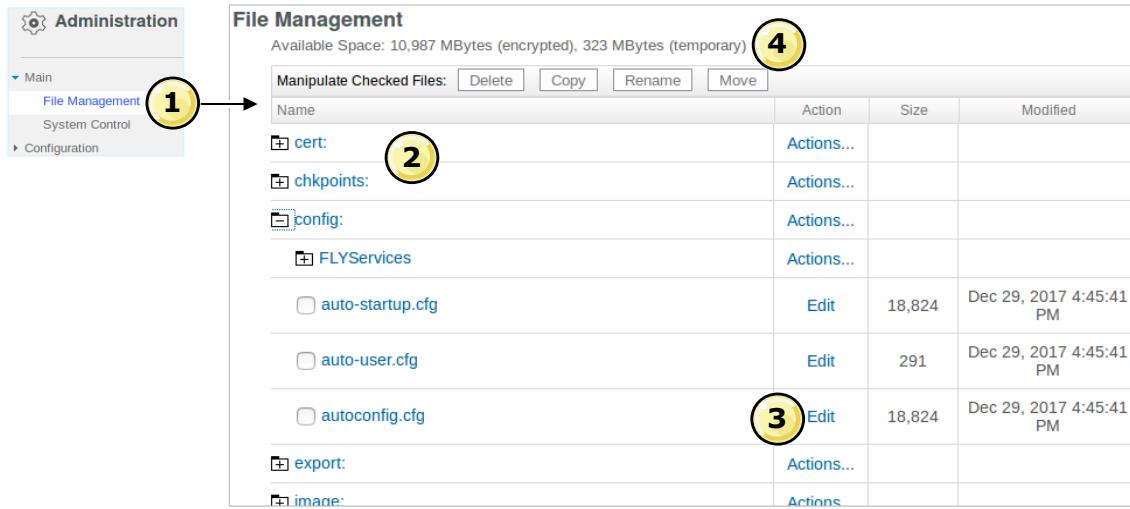
during quiescing. The running configuration contains any changes that were applied while in the quiesced state.

6. **Control Locate LED** controls whether the blue *Locate LED* light on the front of the physical gateway is illuminated. This option is not available on virtual gateways.

# IBM Training



## File management



**File Management**

Available Space: 10,987 MBytes (encrypted), 323 MBytes (temporary)

Name	Action	Size	Modified
cert:	Actions...		
chkpoints:	Actions...		
config:	Actions...		
FLYServices	Actions...		
auto-startup.cfg	Edit	18,824	Dec 29, 2017 4:45:41 PM
auto-user.cfg	Edit	291	Dec 29, 2017 4:45:41 PM
autoconfig.cfg	Edit	18,824	Dec 29, 2017 4:45:41 PM
export:	Actions...		
image:	Actions		

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-12. File management

1. From the navigation bar **Administration** section, select **Main > File Management**.
2. The file stores are divided into different directories. Most directories are specific to one application domain, except for the `store`, `pubcert`, and `sharedcert` directories.
3. Certain files, such as an application domain configuration file, can be directly edited through the web browser.
4. The available space statistics show the amount of nonvolatile memory available for all encrypted data and all temporary data in the system.

There are also hidden `/dp/` directories. They are hidden from view, but occasionally some CLI tasks or some documentation can see them.

## File directories for configuration

Store	Scope	Usage
<b>config:</b>	Per application domain; not shared	Stores configuration files for the current application domain
<b>export:</b>	Per application domain; not shared	Holds any exported configuration that is created with the Export Configuration operation
<b>local:</b>	Per application domain; possibly visible to other domains	Storage space for files that are used by local services, including XML stylesheets and GatewayScript programs <ul style="list-style-type: none"> <li>• Use the <b>visible domains</b> setting to view the local file store of other application domains</li> </ul>
<b>store:</b>	<b>System-wide;</b> shared	Sample and default stylesheets and GatewayScript programs that are used by DataPower services <ul style="list-style-type: none"> <li>• A common practice is to copy these stylesheets and programs into your local directory before you change them</li> </ul>
<b>Temporary:</b>	Per application domain; not shared	Temporary disk space that is used by document processing rules and actions, and is cleared on a gateway restart

Figure 4-13. File directories for configuration

GatewayScript is a DataPower specific implementation of JavaScript.

When auxiliary storage is enabled, it is accessible as a subdirectory of the `local:` and the `logstore:` directories.

## File directories for security

Store	Scope	Usage
<b>cert:</b>	Per application domain; not shared	Location to store private keys and digital certificates <ul style="list-style-type: none"> <li>• System automatically encrypts all files in this store</li> <li>• After being added, files cannot be copied or modified</li> <li>• You can delete digital certificates and private keys</li> </ul>
<b>sharedcert:</b>	<b>System-wide;</b> shared between application domains	Stores digital certificates to be shared with business partners <ul style="list-style-type: none"> <li>• System automatically encrypts all files in this store</li> </ul>
<b>pubcert:</b>	<b>System-wide;</b> shared between application domains	Provides security certificates for root certificate authorities, such as the ones used by web browsers <ul style="list-style-type: none"> <li>• System automatically encrypts all files in this store</li> <li>• Files cannot be modified, but they can be copied</li> </ul>

Figure 4-14. File directories for security

## File directories for logging

Store	Scope	Usage
<b>logtemp:</b>	Per application domain; not shared	Default location of log files, such as the system-wide default log • The file store size is fixed at 13 Mb
<b>logstore:</b>	Per application domain; not shared	Long-term storage space for log files

Figure 4-15. File directories for logging

When auxiliary storage is enabled, it is accessible as a subdirectory of the `local:` and the `logstore:` directories.

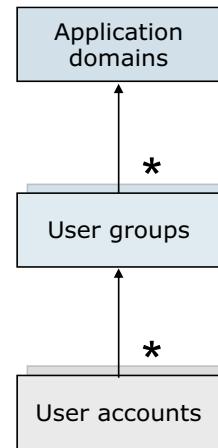
## More file directories

Store	Scope	Usage
<b>audit:</b>	Default domain	Stores the audit log Available from the CLI in the default domain only
<b>checkpoints:</b>	Per application domain; not shared	Contains the checkpoint configuration files
<b>dpcert:</b>	Default domain	Encrypted directory that contains files that are used by the gateway itself Available from CLI in the default domain only
<b>image:</b>	Default domain	Contains the primary and rollback firmware
<b>tasktemplates:</b>	Default domain	XSL files that are used by the WebGUI
<b>isamcert:</b> <b>isamconfig:</b> <b>isamwebroot:</b>	Per application domain	Contains key materials, configurations, and files for IBM Security Access Manager (ISAM) services

Figure 4-16. More file directories

## Administrative access control

- **Application domains** provide a virtualized, enclosed environment for services
  - Only the **default** domain allows administrators to perform system-level tasks, such as configuring an Ethernet interface
- **User groups** apply a specific access policy to a set of user accounts
  - **Privileged** access allows users to perform system-level tasks within the default domain
  - **Group-defined** access relies on a user-defined, fine-grained access policy for each resource
  - **User** access provides read-only, guest access (deprecated)
- **User accounts** provide users with access to the web management interface



*Figure 4-17. Administrative access control*

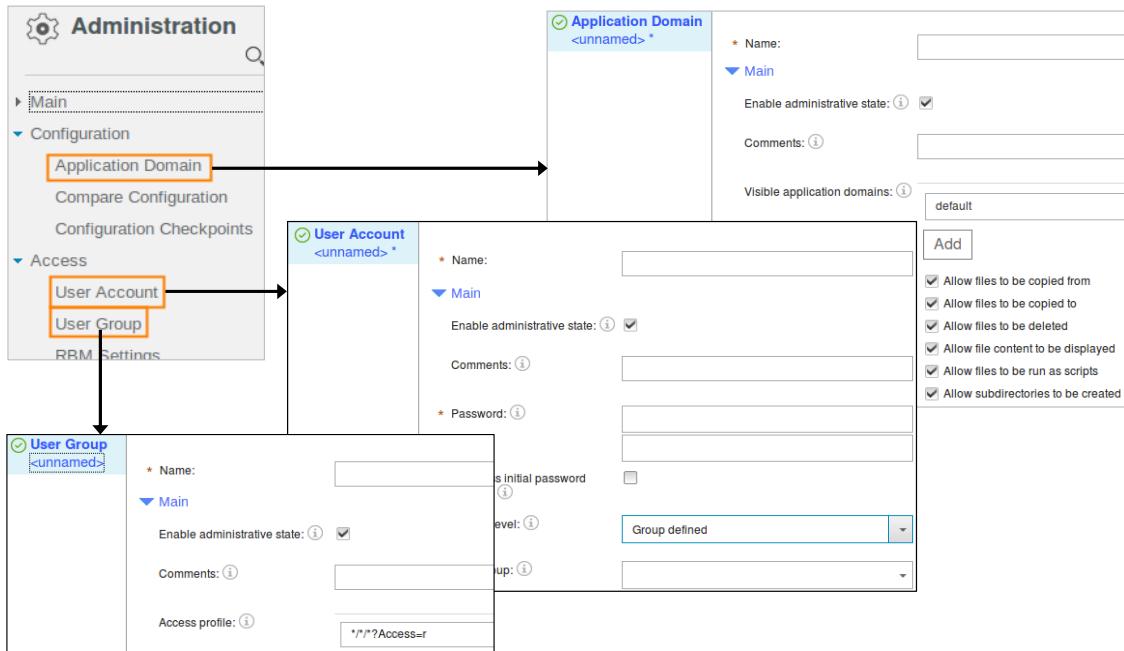
Users can also access more than one application domain, by using the visible domain setting for application domains.

Privileged users are part of the **default** domain until assigned to an application domain. When assigned to an application domain, privileged users are no longer associated with the default domain.

Privileged and user access levels represent the highest and lowest access levels on the DataPower gateway. The group-defined setting allows an administrator to fine-tune the access level within either end of the spectrum.

User accounts that are created through the web management interface apply to the command-line interface (CLI) and XML management interface as well.

## Create application domains, user groups, and users



DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-18. Create application domains, user groups, and users

The Administration section of the navigator bar has links to the wizards for creating application domains, user groups, and user accounts (users).



## Saving configuration changes

**Apply**
**Cancel**

**⚠ Your configuration changes are not saved.**

Click **OK** to continue without saving, or **Cancel** to go back and save your changes.

**OK**
**Cancel**

- Configuration changes take effect after you click **Apply**
  - New configuration exists in memory only
  - A warning window displays when you attempt to switch application domains or log out of web management without saving the applied changes
  
- Click the **Save changes** link that is at the top of the web page to permanently commit any changes

**⚠** The running configuration of the device contains unsaved changes. [Review changes](#). **Save changes**

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-19. Saving configuration changes

The **Apply** submits configuration changes that are made in the current web management page. However, such changes are stored in temporary memory. You must click **Save changes** at the top of the web management interface to commit changes to permanent storage. If you attempt to switch application domains without committing your changes, a warning dialog box is displayed, allowing you to switch domains without saving any changes or to cancel the domain switch.

## Controlling the resource limits of the gateway

- **Administration > Device > Throttle Settings**
- When free memory or file space falls below the **throttle** threshold, the gateway refuses new connections. If enough resource is not freed within the **timeout** period, the gateway restarts.
- When the **terminate** percentage is reached, the gateway restarts
- When the number of free XML Names and JSON Keys reaches the threshold, an alert is written to the log
- The backlog queue holds memory-throttled messages until its timeout expires
  - New requests replace older requests when the backlog size is reached

The screenshot shows a configuration interface for 'Throttle Settings'. It includes fields for:
 

- Memory Throttle At: 20 %
- Memory Terminate At: 5 %
- Temp File Space Throttle At: 0 %
- Temp File Space Terminate At: 0 %
- XML Names and JSON Keys Warn At: 10 %
- Timeout: 30 seconds
- Status Log: (checkbox)
- Environmental Monitor: (checkbox) - checked
- Backlog Size: 0
- Backlog Timeout: 30 seconds

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-20. Controlling the resource limits of the gateway

The throttling process works as follows:

1. *When free memory falls below the throttle threshold* (a measure of free memory that is expressed as a percentage of total memory), the device refuses to accept new connections. By default, the throttle threshold is set to 20 (20% of total memory).
2. If the amount of free memory does not rise above the throttle threshold in the specified timeout (expressed in seconds), the device restarts. By default, the timeout is set to 30 (seconds).
3. *If free memory falls below the terminate threshold* (also a measure of free memory that is expressed as a percentage of total memory), the device restarts immediately. By default, the kill threshold is set to 5 (5% of total memory).

The Temporary file specifications operate the same way.

When the XML namespace reaches 5%, the system restarts. To determine the current state of the XML namespace, go to **Status > XML Processing > XML Names**.

## Notifying on gateway failure

- Administration > Device > Failure Notification
- Sends an error report on the restart of the gateway after a failure
- Clear the E-mail Notification and select Upload Error Report to get the most flexible error report contents
- The choices for report destination are
  - FTP
  - NFS
  - RAID volume on the gateway
  - SMTP (email)
  - temporary: directory
- The page refreshes to provide the particular specifications, depending on the protocol selected

The screenshot shows a configuration interface for 'Failure Notification' under the 'Main' section. It includes the following fields:

- Enable administrative state:
- Comments:
- Upload Error Report:
- Include Internal State:
- Background Packet Capture:
- Background Log Capture:
- Background Memory Trace:
- Always On Startup:
- Always On Shutdown:
- \* Report Destination Protocol:
- \* FTP Server:
- FTP Path:

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-21. Notifying on gateway failure

The fields on the page change as different choices are made.

Initially, the two primary choices, **Upload Error Report** and **Email Notification**, are off.

Even if you want email notification, the best approach is to clear **Email Notification**, and select **Upload Error Report**. This approach gives you more options to specify for the contents of the error report, and still allows you to select an email destination.

If you set **Email Notification** to on, the **Upload Error Report** choice disappears, and fields for specifying an email destination are shown.

A background log capture is a continuously running log capture with low use of system resources. This capture is in addition to the standard log and trace entries.

A background memory trace enables automatic memory leak detection when the memory on the gateway gets low.

The background packet capture is a continuously running network packet capture on all Ethernet interfaces.

## Administration by using the command-line interface

- The command-line interface (CLI) provides a text terminal for administering the DataPower gateway
  - For security purposes, the CLI is not a complete command shell with the ability to run arbitrary programs
  - You can configure every service and interface available in the DataPower gateway with the CLI
  - In the initial setup, you must enable the web management interface and Ethernet ports with the CLI through a serial connection
  - Administrators have the option of enabling the CLI over a Telnet or Secure Shell (SSH) connection

Figure 4-22. Administration by using the command-line interface

The CLI is not a complete command shell with the ability to run arbitrary programs.

However, the CLI allows you to configure every service and interface available in the DataPower gateway.

In the initial setup, you must enable the web management interface and Ethernet ports with the CLI through a serial connection.

## Administration by using the XML Management Interface

- DataPower gateways accept administration commands by using XML messages
  - SOAP Configuration Management (SOMA)
  - Appliance Management Protocol (AMP)
  - Service Level Management (SLM)
  - WS-Management and Web Services Distributed Management (WSDM)
- Each API has its own endpoint URI
- Most commonly used XML Management interfaces are SOMA and AMP

Figure 4-23. Administration by using the XML Management Interface

DataPower gateways accept administration commands by using XML messages.

These APIs can be changed with XML messages:

- SOAP Configuration Management (SOMA)
- Appliance Management Protocol (AMP)
- Service Level Management (SLM)
- WS-Management and Web Services Distributed Management (WSDM).

Each API has its own endpoint URI.

## Administration by using the REST Management Interface

- Provides access to the actions and to the configuration and status resources on the gateway
  - Retrieve status or configuration data
  - Create, modify, or delete a configuration
  - Run actions
- Similar to the SOAP management interface, but with a REST HTTP calls and JSON data

*Figure 4-24. Administration by using the REST Management Interface*

You can administer the gateway by using the REST Management Interface.

The REST management interface uses HTTP calls with JSON messages.

## Management interface summary

- Web management interface:
  - Easy-to-use interface accessible through a web browser
    - WebGUI (traditional)
    - Blueprint Console (replacing WebGUI)
  - Built-in online help for fields and operations
  - **Apply** and **save** steps allow administrators to discard or save any changes after testing
- Command-line interface (CLI):
  - The only interface that is initially enabled
  - Simple environment that is similar to UNIX
- XML management interface:
  - Allows the configuration of an application domain, or the entire gateway, through a batch of commands
  - Multiple APIs allow third-party applications to manage the gateway
- REST management interface:
  - Similar to SOAP management but uses REST HTTP calls with JSON-structured data

Figure 4-25. Management interface summary

This page summarizes the different management interfaces and how they are used.

## Appliance and services status



### What is available?

- Active services
- Object status
- TCP port status
- Ethernet interfaces



### How is the gateway?

- CPU usage
- File system information
- Memory usage
- System usage
- Transaction rate
- Environmental sensors
- Ethernet interfaces

Status information is collected and displayed by **status providers**

- Who am I?
  - Firmware information
  - Library information
  - Licensing information
  - System settings
- What is using the memory?
  - Service-wide
  - Transaction-level

*Figure 4-26. Appliance and services status*

The same information is also available from CLI commands.

## Secure backup mode

- Secure backup mode is available only if you enabled secure backup mode during the initial firmware setup of the gateway
  - If not enabled, you must reinitialize the gateway to enable the secure backup mode
- Secure backup mode creates a secure backup to recover the configuration of a gateway
  - A secure backup contains private data from the gateway, including certificates, keys, and user data
  - Normal backup does **not** include the key materials
- Only a DataPower gateway can decrypt the data in the backup
  - A person or a tool cannot read the data
- Secure backup mode must be enabled to create secure backups for use after a gateway failure or during an end of life migration

*Figure 4-27. Secure backup mode*

Secure backup mode is set during the initialization of the gateway. During the initialization of the gateway, the user is prompted to enable secure backup mode. Answering “yes” sets the secure backup mode, allowing the secure backup process to be initiated. Answering “no” sets the gateway to normal mode, disallowing initialization of the secure backup process. When the secure backup mode is set, it cannot be reset unless the device is reinitialized.

Good practices:

- If required, select secure backup mode at initialization time.
- Do not start backups while configuration, style sheet, or other changes are in progress.
- Save all configurations before backup.
- System activity affects time that is required for a backup.
- Back up during low system usage.
- Avoid backing up RAID and iSCSI, if not required, because of size and network impact.
- The private key of the public certificate is required at restore time.
- Back up at each firmware upgrade or gateway application modification.



## Determining current Backup mode

### Administration > Device > System Settings

- Backup Mode
  - Normal
  - Secure

### CLI

- Show system

The mode is read-only and you must reinitialize to change the mode

Product OID:	<input type="text" value="1.3.6.1.4.1.14685.1.8"/>
Description:	<input type="text" value="IBM DataPower Gateway"/>
Serial number:	<input type="text" value="0000000"/>
Entitlement serial number:	<input type="text" value="0000000"/>
Product ID:	<input type="text" value="5725 [Rev None]"/>
Contact:	<input type="text"/>
Appliance name:	<input type="text" value="DP50-IDG-760"/>
Location:	<input type="text"/>
Services:	<input type="text" value="72"/>
Backup mode:	<input style="border: 2px solid red;" type="text" value="Secure backup"/>
Product Mode:	<input type="text" value="Normal"/>

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-28. Determining current Backup mode

To determine whether an gateway is in secure backup mode from either the CLI or web management, the following steps are taken.

From the CLI, show the system configuration: `co; show system`. The backup mode is either “normal” or “secure.” A gateway in normal backup mode is not in secure backup mode and cannot start a secure backup. A gateway in secure backup mode is in secure backup mode and can start a secure backup.

The same information is shown in web management from the **Administration > Device > System Settings** panel.



## Perform a secure backup

- Web management:
  - Administration > Main > System Control > Secure Backup
- CLI:
  - `secure-backup certName destination [include-raid]`
  - `secure-backup myCert ftp://9.1.2.3/backups off`

Specify:

- Certificate for encrypting
- Backup file destination
- Whether to include the contents of the RAID volume
  - Default is **on**

The screenshot shows two stacked configuration panels. The top panel is titled 'Secure Backup' and contains fields for 'Crypto certificate' (set to '(none)'), 'Destination' (a text input field), and 'Include RAID' (a radio button set to 'on'). The bottom panel is titled 'Secure Restore' and contains fields for 'Crypto credentials' (set to '(none)'), 'Source' (a text input field), and 'Only validate the backup' (a radio button set to 'off'). Both panels have a 'Secure Backup' or 'Secure Restore' button at the bottom.

[DataPower administration overview](#)

© Copyright IBM Corporation 2018

Figure 4-29. Perform a secure backup

The certificate that is used to encrypt the secure backup file must not use an ESDSA key.

Secure backups can be written to the local: or temporary: directories, or to an FTP destination.

A secure backup operation does not include the contents of the hardware security module (HSM), if present.

## Restoring a gateway (1 of 3)

Secure restores are destructive:

- Existing data on the target gateway is lost
- Data is replaced and not merged

The target gateway must be compatible:

- Same firmware level as the backup
- Same storage devices (compact flash, iSCSI, and RAID)
- At least as much storage capacity on each device

After it is restored, a gateway requires some configuration before being used

- The password for the **admin** account is reset to *admin* and must be changed
- Network information must be changed if the target gateway moved
- Restore RAID devices when backed up by using another method
  - Configuration information about the RAID might need to be updated

A secure restore validate option is available

- Reads only the manifest file
- Verifies compatibility but does not check data files or gateway storage capacity
- Does not delete data from the target gateway
- Useful to validate secure backup procedures

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-30. Restoring a gateway (1 of 3)

The secure restore is a destructive process. Any data on the gateway that is restored is viewed as temporary, and the backup date replaces the data on the gateway. For example, the network information about the gateway is required to restore the backup. But after the backup is complete, the network information from the files that were backed up will be on the gateway.

The target gateway must be “compatible.” This requirement means that it must be at the identical firmware level. The storage devices must be the same and have at least as much capacity as the backed up gateway.

After an gateway is restored, the administrator must log in as **admin** and change the password from the default *admin*. This procedure ensures that the installation has at least one administrator with a known password. Also, network data might need to be changed if the gateway moved since the backup. RAID devices are required to be compatible for the restore to be successful. Verify their configuration to ensure that the backup configuration for the devices is correct.

It is important to note that the private key pair of the public certificate is required at restore time. Without the private key, no one can view or use the backed up data.

The validate option is useful to check that a backup exists before a disaster happens. It validates just the manifest file information without reading the backed up data or deleting the data on the gateway.

After a restore is complete, the administrator **must** log in with the admin ID and change its password. Verification of network and RAID configurations also ensures that the gateway restore is successful.

## Restoring a gateway (2 of 3)

- You must create the credentials that the secure restore process uses on the gateway that is being restored
- Secure backup/restore is not supported between physical and virtual gateways
- The following restores for physical gateways are supported:
  - XG45 to XG45 or IDG
  - XI52 to XI52 or IDG
  - XB62 to XB62 or IDG
  - IDG to IDG
- The following restores for virtual gateways are supported:
  - Production to a production, nonproduction, or developers
  - Nonproduction to a production, nonproduction, or developers
  - Developers to a production, nonproduction, or developers

Figure 4-31. Restoring a gateway (2 of 3)

Secure backup and restore is not supported across physical and virtual gateways.

You can use a backup image from a virtual DataPower gateway to restore a virtual DataPower gateway.

## Restoring a gateway (3 of 3)

- Web management:
  - Administration > Main > System Control > Secure Restore
- CLI:
  - `secure-restore idCredName source [validate] [backup-machine-type]`
  - `secure-restore myIdCred ftp://9.1.2.3/backups off`

### Specify:

- Crypto identification credential
  - Points to the encrypting certificate and the associated private key
- Backup file location
- Whether to validate the backup file, rather than restore it
  - Default is **off**

The figure consists of two side-by-side screenshots of the IBM DataPower administration interface. The left screenshot, titled 'Secure Backup', shows fields for 'Crypto certificate' (dropdown with '(none)'), 'Destination' (text input), and 'Include RAID' (radio buttons 'on' and 'off'). The right screenshot, titled 'Secure Restore', shows fields for 'Crypto credentials' (dropdown with '(none)'), 'Source' (text input), and options for 'Only validate the backup' (radio buttons 'on' and 'off', with 'off' selected) and 'Backup appliance model' (text input). Both screenshots have a 'Secure Backup' or 'Secure Restore' button at the bottom.

DataPower administration overview

© Copyright IBM Corporation 2018

Figure 4-32. Restoring a gateway (3 of 3)

The certificate that is used to encrypt the secure backup file must not use an ESDSA key.

Secure backups can be written to the local: or temporary: directories, or to an FTP destination.

A secure backup operation does not include the contents of the hardware security module (HSM), if present.

The machine types are:

- IBM DataPower Gateway (IDG) - 843652X (without HSM), 843653X (with HSM)
- DataPower Service Gateway (XG45) - 719832X
- DataPower Integration Appliance (XI52) - 719942X
- DataPower B2B Appliance (XB62) - 719962X
- DataPower Gateway Virtual Edition - 5725T09

The machine type for the backed-up gateway can be seen in the manifest file of the secure backup.

## Quiescence

The quiesce process changes the operational state of the gateway's domains, services, and handlers to shut down in a controlled manner.

- Finer grained quiescence includes:
  - Domains
  - Services
  - Protocol handlers

Management commands to:

- Quiesce
  - Stop new requests on the front side
  - Allow the current requests to complete
  - Notify when there are no more requests in progress (or Quiesce times out)
- Unquiesce
  - Restart services that are involved in quiesce

Quiesce and Unquiesce commands are available for:

- Front-end handlers
- Services
- Domains
- Gateway

DataPower administration overview

© Copyright IBM Corporation 2018

*Figure 4-33. Quiescence*

Broadly, the purpose of quiesce is to stop traffic on a set of services in a controlled manner. Quiesce stops new requests from being processed and allows ongoing requests to complete. At the end of quiesce, a notification is issued.

Quiescing is important because it is used to drain traffic from the gateway for production deployment.

Unquiesce is complementary to quiesce and restarts services.

Quiesce and unquiesce are actions on Front Side Handlers, services, domains, and at the gateway level.

## Unit summary

- List the methods that can be used to administer the DataPower appliance
- Work with files on the DataPower appliance
- Determine the status of various aspects of the appliance
- Run secure backup and restore
- Quiesce traffic to the appliance

Figure 4-34. Unit summary

## Review questions

- 1. True or False:** One way to restrict access to an application domain is to define user groups to restrict user account access to a particular domain.
- 2.** Which user account do you need to use to perform a firmware upgrade?
  - A. user00
  - B. Any user account
  - C. Linux root
  - D. admin
- 3.** Match the advantages in performing administration tasks with the various DataPower management interfaces:

Description	Definition
1. The WebGUI web application	A. Creation of scripts, less bandwidth
2. The command-line interface (CLI)	B. Easier to use
3. The XML Management Interface	C. Programmatic

Figure 4-35. Review questions

Write your answers here:

- 1.
- 2.
3.
  - (1)
  - (2)
  - (3)

## Review answers

1. **True.** One way to restrict access to an application domain is to define user groups to restrict user account access to a particular domain.
2. **D.** Which user account do you need to use to perform a firmware upgrade?
  - A. user00
  - B. Any user account
  - C. Linux root
  - D. admin**

3. Match the advantages in performing administration tasks with the various DataPower management interfaces:

Description	Definition
1. The WebGUI web application	<b>B. Easier to use</b>
2. The command-line interface (CLI)	<b>A. Creation of scripts, less bandwidth</b>
3. The XML Management Interface	<b>C. Programmatic</b>

Figure 4-36. Review answers

---

# Unit 5. Using CLI and the XML Management Interface to configure appliance

## Estimated time

01:30

## Overview

This unit focuses on the non-browser approach to defining appliance and service resources. It begins with the traditional text-based approach, the command-line interface (CLI). It reviews basic syntax and commands, provides examples of resource configuration, and explains several of the ways to control CLI access. The unit then reviews the SOAP configuration management (SOMA) approach, explaining basic syntax and providing examples of XML Management Interface requests and responses. Lastly, the unit explains Appliance Management Protocol (AMP) and its syntax.

## How you will check your progress

- Review questions
- Lab exercise

## References

IBM DataPower Gateways Version 7.6.0 product documentation:

[http://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0](http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0)

## Unit objectives

- Compare and contrast the DataPower management approaches: CLI, XML Management Interface, and the WebGUI
- Use CLI to configure domains, user groups, and users
- Configure administrative and development access to the appliance and resources
- Issue CLI commands to define and manage network resources
- Construct SOAP configuration management (SOMA) requests
- Use SOMA requests to configure resources and perform management functions
- Construct Appliance Management Protocol (AMP) requests
- Use AMP requests to run management functions

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-1. Unit objectives

## Administrative interfaces

- CLI (command-line interface)
  - Typical command-line interface over a serial connection or Ethernet
  - Required for the initial appliance configuration, or an appliance reinitialization
  - Might be the only option when the appliance is having network or response time issues
- XML Management Interface (XMI)
  - Many endpoint interfaces for XML-based management requests
  - Common endpoints are SOAP-based configuration management (SOMA) and Appliance Management Protocol (AMP)
  - Easy to build scripts to automate a configuration
- REST Management Interface (RMI)
  - Similar capabilities as SOMA
  - Uses typical RESTful interactions with JSON request/response payloads
- Web Management Interface
  - Browser-based interface (WebGUI and Blueprint Console)
  - Easy to use for the novice: Menus, navigation bar, field prompts, and online help

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-2. Administrative interfaces

## Enable the SSH CLI interface

- CLI access over a serial console connection is always enabled
- CLI access over an Ethernet interface is initially disabled
- One of first tasks during initialization or reinitialization is to enable the SSH service:
  - CLI: `ssh ip-address port-number`
  - Web management: Select **Network > Management > SSH Service**

**SSH Service**

Status: up

▼ Main

Enable administrative state:

\* Local address:

\* Port number:

Access control list:

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-3. Enable the SSH CLI interface

This service is disabled by default. When setting up the gateway for the first time, make sure that you enable this service, along with the web management interface.

The **Local IP address** specifies the Ethernet interface on the appliance that the service listens to for requests. For security, a good practice is to restrict access to this service to the management Ethernet interface. Do not allow access to this service from all Ethernet interfaces (0.0.0.0).

The certificate that is used is the gateway certificate (default that is supplied, or regenerated).

## CLI users

Users must have permissions to access the CLI interface.

- The user ID **admin** is always allowed access to CLI

Assignment of CLI permissions is accomplished by using one of the following objects:

- User account
  - Assign the user group **privileged**
  - Restrict access to specific domains
- User group
  - Access to sets of CLI commands
  - Define an access profile
- RBM settings
  - “Enforce RBM on CLI” option
- Access profile that is composed of one or more access policies
  - Access policy defines access to specific configuration and action objects, and specific permissions on the allowed objects



Figure 5-4. CLI users

The **admin** user is the default user account that always exists. It is similar to **root** in a Linux or UNIX environment.

**RBM** is role based management.

Role-based management provides a flexible and integrated way to control whether an authenticated user has the necessary permission to access resources through access policies.



## RBM settings and CLI

### Administration > Access > RBM Settings

Enforce RBM on CLI:

- off
  - Available CLI commands are defined in user group “CLI command groups”
  - Available domains are defined in user account “domain restriction”
- on
  - User group “access profiles” controls the access permissions

When the RBM Settings object is disabled, its settings do not apply to CLI access

- The following users can then access the CLI:
  - Users with the **privileged** access level
  - **User group**-defined users with permissions to command groups

**RBM Settings**

Status: up

▼ Main

Enable administrative state:

▶ Authentication

▶ Credential-mapping

▶ Password policy

▼ Account policy

Restrict admin to serial:

\* Maximum failed logins:

Lockout duration:

Enforce RBM on CLI:

[Using CLI and the XML Management Interface to configure appliance access](#)

© Copyright IBM Corporation 2018

Figure 5-5. RBM settings and CLI

**RBM** is role based management.

When the RBM Settings enable administrative state is unchecked in the Blueprint Console, its settings do not apply to CLI access

The following users can then access the CLI:

Users with the **privileged** access level

**User group**-defined users with permissions to command groups

## Controlling access in a User Account object

- Assign the **Access Level**

- Privileged:** Grants access to all of the CLI commands in one or more domains (depends on the Domain Restriction list)
- Group-Defined:** Indicates that a user group defines the access that a particular user is granted

Name	Op-State	Access level	User group
<input type="checkbox"/> admin	up	privileged	
<input type="checkbox"/> student95	up	group-defined	student95_developer_group
<input type="checkbox"/> sysadmin	up	privileged	

Figure 5-6. Controlling access in a User Account object

User account “access level” choices are **Group-Defined**, **Privileged**, and **User**.

**User** restricts the account to status information only and is deprecated.

## Controlling access in a User Group object

- Define **access profiles** to domains, configuration objects, and action objects
  - Particular permissions in these domains and on these objects
- Restrict the user group to sets of CLI commands
  - On lower part of page
- CLI Command Groups do **not** equate to access profiles

The screenshot shows the 'Main' tab of a User Group configuration screen. It includes fields for Name (student95\_developer\_group), Enable administrative state (checked), and Comments (Developer group for the student 95 domain). The 'Access profile:' section contains three entries: \*/student95\_domain/\*?Ao, \*/student95\_import\_doma, and \*/student95\_remote\_dom;. An 'Add' button is available below this list. To the right of each entry is a 'Build' dropdown menu, all set to 'Build'. The 'Command group:' section contains a single entry 'AAA Policy' in a dropdown menu, with an 'Add' button below it.

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-7. Controlling access in a User Group object

The Build link that is displayed in the screen capture enables you to edit the access property for the user group.

In the pop-up window for the Build, you can specify the application domain and privileges in the access profile.

Privileges include read, write, add, delete, and execute options.

## Global configuration mode

- Use the command **configure terminal** to enter the global configuration mode:
  - Create and configure system-wide resources
  - Enter other configuration modes
  
- Switch domains by using the **switch domain [domain-name]** command
- Perform create, retrieve, update, and delete operations on objects:
  - Enter the respective object configuration mode to *create* an object
  - Retrieve information about objects by using the **show** command
  - Delete configuration objects by using the **no** command
  - Enter the respective object configuration mode to *update* an object

```
idg# configure terminal
Global configuration mode
idg(config)# ethernet eth0
```

Figure 5-8. Global configuration mode

The shortcut **co** can be used instead of **configure terminal**.

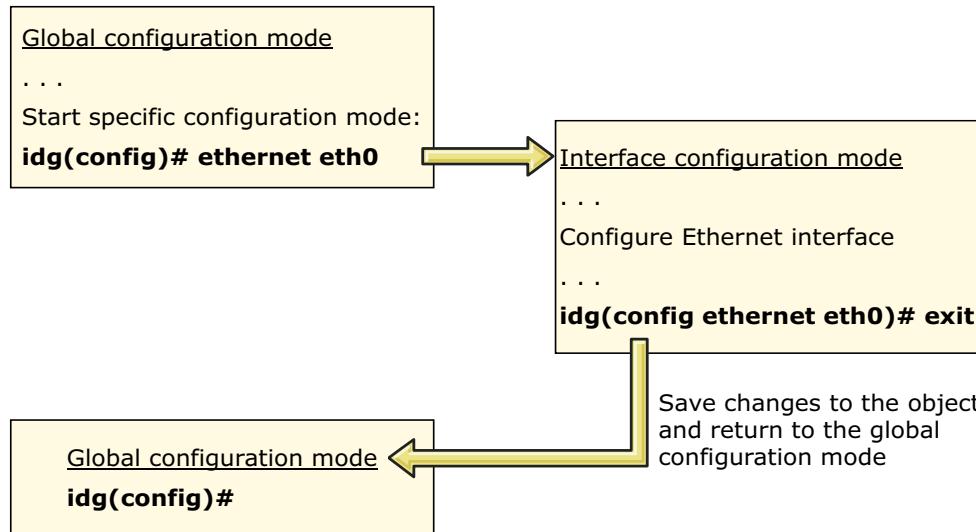
In the global configuration mode, the administrator can create, modify, or remove any DataPower service or interface that can be found in the Web Management service.

The examples in this presentation use the default domain. You are likely to create objects in various domains. Use the “**switch domain [domain name]**” command to switch to another domain. The CLI prompt indicates the current domain in square brackets, for example: **idg [domain-name] (config-crypto)#[/b]**

The absence of a domain name indicates the default domain.

## Entering and leaving a configuration mode (1 of 2)

- Use the configuration mode name and the object name to enter
- Use **exit** to commit any changes



Using CLI and the XML Management Interface to configure appliance access

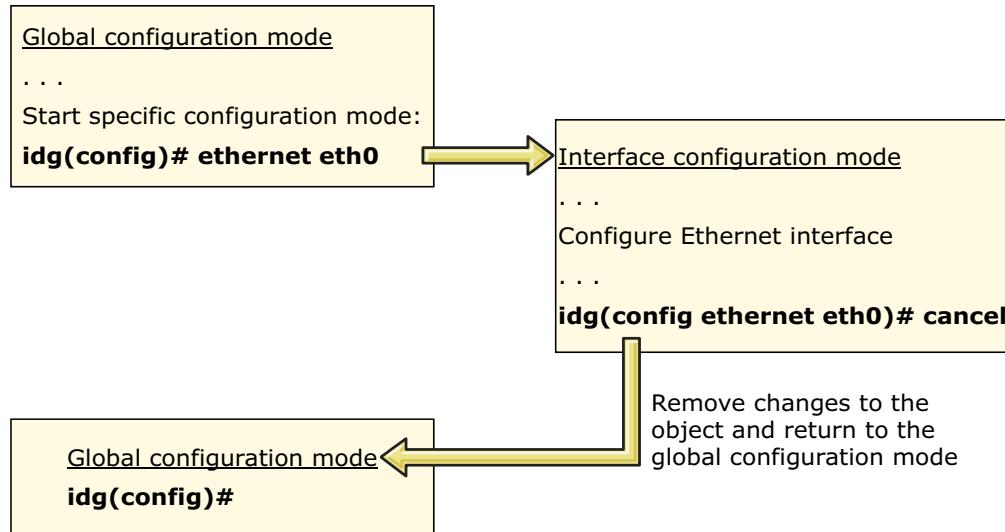
© Copyright IBM Corporation 2018

Figure 5-9. Entering and leaving a configuration mode (1 of 2)

The “eth0” Ethernet interface configuration is created and saved when you **exit** out of the “Ethernet” configuration mode.

## Entering and leaving a configuration mode (2 of 2)

- Use **cancel** to leave the specific configuration mode and ignore changes



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-10. Entering and leaving a configuration mode (2 of 2)*

Use **cancel** to leave the configuration mode and to ignore any changes that are entered while in the mode.

## Create and update objects over CLI

- Enter a respective object configuration mode from the global configuration mode
  - Entering a **new** object name *creates* an object
  - Entering an **existing** object name allows you to *update* the object properties
- Example:

- Specify the name for the new object (HTTP protocol handler for example):

```
idg(config)# switch domain test
idg[test] (config)# source-http myhttpandler
idg[test] (config source-http myhttpandler)#+
```

- Assign the listening **port** for the HTTP handler, and save:

```
idg[test] (config source-http myhttpandler)#
 port 6780
idg[test] (config source-http myhttpandler)#
 exit
```

Figure 5-11. Create and update objects over CLI

An HTTP protocol handler defines the listening IP address and port for a service.

The HTTP protocol handler is created when you **exit** out of the `source-http` configuration mode.

- Not entering a name for an object results in the creation of an object with a system-assigned name.
- Use the `help` command to view configurable object properties.
- Use the `show` command to view object attributes that are already set.

## Common commands

- Networking and Ethernet interfaces
  - Manage the IP configuration of the appliance interfaces
  - Configure the DNS settings
- Monitoring and troubleshooting
  - Show current users and TCP connections
  - Debug networking issues by using `route`, `ping`, and `tcp-connection`
- Backup
  - Back up the domain: `export [file-name] [domain]`
- Help system
  - Type `help` or `?` on the command line
  - Type `help show` to get help on a specific command
  - Context sensitive
- Save configuration (same as the **Save Configuration** feature in the WebGUI)
  - Use the command `write memory`
- `exit` leaves the current configuration mode and returns to the parent mode
  - Applies changes to the objects made in the object configuration mode
- `cancel` leaves the current configuration mode and returns to the parent mode
  - Removes changes to the objects made in the object configuration mode

Using CLI and the XML Management Interface to configure appliance  
access

© Copyright IBM Corporation 2018

Figure 5-12. Common commands

The command `write memory` can be abbreviated as: `write mem`

## Retrieve system information by using CLI

- **show version**
  - Returns the serial number, firmware level and build date, XML accelerator version, and any libraries
- **show services**
  - Returns a list of all active DataPower services and their respective ports
- **show users**
  - Lists all users that are currently logged in to the device
- **show log**
  - Returns the default log file
- **show audit-log**
  - Returns the audit log file
- **show startup-config**
  - Displays the configuration, in CLI commands, for which the device was most recently booted or restarted
- **show route**
  - Displays the device routing table

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-13. Retrieve system information by using CLI

Use the `show` command to retrieve information about an appropriate object.

Use the command `show startup-errors` to view any errors in the startup configuration. This command is helpful when debugging issues in the `startup-config` file.

To show the `audit-log` and the `startup-config`, you must be in the global configuration mode.

Use `show running-config` to view the currently saved configuration mode.

## Ethernet interfaces (1 of 2)

- View a list of all appliance interfaces:
  - Use the command **show network-interface**

ifIndex	Type	Name	Administrative status	Operational status	IP version	IP address			
ops			Prefix length	MAC address	MTU	RX bytes	RX packets	RX errors	RX drops
TX bytes				TX errors	TX drops				
1	Other	lo	up	up		127.0.0.1			
			8	00:00:00:00:00:00	16436	592276148	3194129	0	0
2	592276148	3194129		0	0				
2	Other	gre0	down	lowerLayerDown		ipv4			
			0	00:00:00:00:00:00	1476	0	0	0	0
0	0	0	0	0					

- Change and set the IP address that is assigned to an appliance interface

```
idg (config) # interface mgt0
Interface configuration mode (mgt0)
idg (config-if[mgt0]) # ip address 10.10.11.214/23
idg (config-if[mgt0]) # ip default-gateway 10.10.10.1/23
idg (config-if[mgt0]) # exit
```



Ethernet interfaces

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-14. Ethernet interfaces (1 of 2)

This information is also available in the WebGUI (**Network > Interface > Ethernet Interface**).

The action of **write mem** persists the changes to the appliance flash memory. If you restart the appliance without running the **save mem** command, your changes are lost.

The default gateway is a node on the network that allows access to another network.

The user must be in the default domain to run the **interface** command and configure appliance IP addresses.

The interfaces on the DataPower appliance are typically assigned static IP addresses, although dynamic IP addresses are also supported.

The appliance has multiple network interface cards (NIC), dependent on model, which can be assigned unique IP addresses.

Although management and client traffic can occur with any interface, one interface is usually designated as a management interface. All of the appliance management traffic is configured to use that IP address. There are several interfaces on the appliance that are named as management interfaces to reinforce this approach.

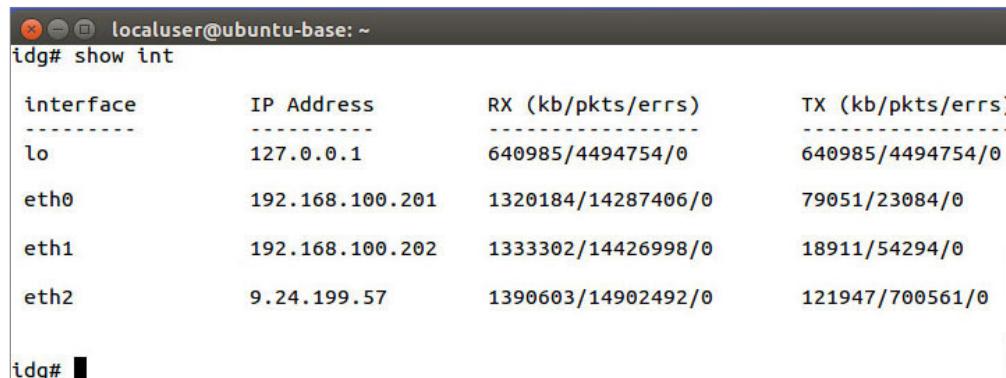
Do not change the IP configuration of the management interface by using SSH or the WebGUI, unless you already specified “all interfaces” (0.0.0.0) for your CLI, XMI, or WebGUI management

interfaces. Otherwise, after you change the configuration, you are unable to access the appliance because the connection is broken after the change.

You can enable or disable an interface. This ability is useful during debugging because it allows you to stop Ethernet traffic on an interface without having to physically unplug a cable.

## Ethernet interfaces (2 of 2)

- Virtual appliances can have eth0, eth1, eth2, and eth3 Ethernet interfaces defined



interface	IP Address	RX (kb/pkts/errs)	TX (kb/pkts/errs)
lo	127.0.0.1	640985/4494754/0	640985/4494754/0
eth0	192.168.100.201	1320184/14287406/0	79051/23084/0
eth1	192.168.100.202	1333302/14426998/0	18911/54294/0
eth2	9.24.199.57	1390603/14902492/0	121947/700561/0

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-15. Ethernet interfaces (2 of 2)

In the example on the page, a virtual appliance has been accessed with SSH and the **show interface** CLI command is run.

## Associate Ethernet interface to administrative service

- A common security practice is to limit access to administrative services only to a management Ethernet interface
  - WebGUI (9090)
  - SSH (22)
  - XML Management Interface (5550)
- Restricts administrative access at the network layer
  - Avoid using the IP address **0.0.0.0** because it allows access from all Ethernet interfaces

```
idg(config)# web-mgmt 10.26.47.8 9090
Web management: successfully started
idg(config)# ssh 10.26.47.8 22

% Pending

SSH service listener enabled
idg(config)# exit
idg#
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-16. Associate Ethernet interface to administrative service

These commands associate the IP address 10.26.47.8 to the Web Management and SSH services. These services cannot be accessed through any other IP address, even though the appliance has other NIC cards.

The port numbers that are listed are the defaults.

## Network utilities

- Configure DNS settings:

```
idg(config)# help ip domain
Options:
 ip name-server Identifies a DNS server
 ip host Defines a host-name to IP-address mapping
 ip domain Adds an entry to the IP domain table

idg(config)# ip domain dp.ibm.com
idg(config)# ip host localhost 127.0.0.1
idg(config)# ip name-server 10.26.46.4
```

- idg(config)# show route

destination	interface	gateway	metric
0.0.0.0/0	mgt0	10.26.46.1	0
10.26.46.0/23	mgt0		0

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-17. Network utilities

View the DNS configurations in the WebGUI at **Network > Interface > DNS Settings**.

The DNS settings allow you to add a DNS name server, domain prefix (appends a string to a host without a fully qualified domain name), and a static host.

The **metric** field in the routing table identifies the cost or number of hops to the gateway. The example on the figure contains a metric value of 0 because the appliance is directly connected to the gateway. The routing table algorithm uses the value to determine the quickest path to a gateway.

The destination 0.0.0.0 in the routing table is the default route if no matches are found.

## Monitoring commands

- List of current TCP connections: **show tcp**

```
idg(config)# show tcp

local address remote address state
----- -----
0.0.0.0:22 0.0.0.0:0 listen
0.0.0.0:80 0.0.0.0:0 listen
...
```

- List of currently logged-in users: **show users**

```
idg(config)# show users

Session ID Name Connection IP address Login Domain
----- ----- -----
3 admin serial-port Mon Mar 19 18:28:59 2018
 default
34 admin secure-shell 192.168.100.200 Fri Apr 6 13:54:40 2018
 default
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-18. Monitoring commands*

The **show users** command also shows the time of login, for example:

Fri Apr 6 13:54:40 2018

## Troubleshooting commands

- Send an ICMP echo request packet to host: **ping**
  - Test whether the destination address can be reached from the appliance

```
idg(config)# ping appserver.dev.datapower.com
PING appserver.dev.datapower.com (10.26.69.156) with 56 data bytes of data
64 bytes from 10.26.69.156: seq=0, ttl=127, rtt=1.0 ms
64 bytes from 10.26.69.156: seq=1, ttl=127, rtt=1.0 ms
64 bytes from 10.26.69.156: seq=2, ttl=127, rtt=2.0 ms
3 packets transmitted, 3 received, 0% loss, time 4005 ms
```

- TCP connection test: **test tcp-connection [host] [port]**

```
idg(config)# test tcp-connection appserver.dev.datapower.com 9080
TCP connection successful
```

Figure 5-19. Troubleshooting commands

Although an IP address is reachable, an intervening router or firewall can block ICMP requests that cause **ping** to fail.

These functions are the same as you find in the troubleshooting page of the WebGUI.

## Scripting commands

Administrators can use the CLI interface to run CLI scripts that perform tasks in a repeated and auditable way.

The following commands are useful in building and running scripts:

- **alias**: Creates a shortcut to a set of commands
- **copy**: Copies a file to and from the appliance
  - Several transport protocols are supported
- **exec**: Runs a target configuration script

*Figure 5-20. Scripting commands*

The `copy` command supports the following transport protocols: HTTP, HTTPS, SMTP, SCP, and SFTP.

## Alias command

- Use the command **alias** to create shortcuts for a set of commands:
  - **alias <alias-name> <set of commands>**
  - Separate multiple commands by using a semicolon ( ; )
  - Single command alias

```
idg(config)# alias save write mem
idg(config)# save
Overwrite previously saved configuration [y/n]? y
```
  - Multiple command alias

```
idg(config)# top
idg# alias mgtport 'configure terminal;interface mgt0'
idg# mgtport
Global configuration mode
Interface configuration mode (mgt0)
idg(config-if[eth4])#
```

Figure 5-21. Alias command

Use the **show aliases** command to display all aliases.

## Copying files

- Copies files from other servers to the local file system
  - Supports the following transport protocols: HTTP, HTTPS, SMTP, SCP, and SFTP
  - There is no “file upload” in the SSH CLI session, so the **copy** command is the way to get a file onto the appliance

```
idg(config)# help copy
copy [-f] <source-URL> <destination-URL>

idg(config)# copy http://host/image.crypt image:///image.crypt
file copy successful (1534897 bytes transferred)
```

- To view the file system contents, use the command  
**dir <file-directory>**:

Figure 5-22. Copying files

The file system has a limited capacity and is best used to store style sheets and configuration files. The **-f** flag in the **copy** command forces files to be overwritten without user interaction.

## The exec command

The **exec** command calls and runs a configuration script.

- Scripts can be run within another configuration script

The **exec** command enables the modularization of configuration scripts

- Scripts for different tasks
- Example: Use **main.cfg** to call the following
  - Interface script: **interfaces.cfg**
  - Services script: **services.cfg**

```
idg # configure terminal
idg(config)# help exec
exec <local-url>

idg(config)# exec config:///interfaces.cfg
idg(config)# exec config:///services.cfg
```

Figure 5-23. The exec command

## User and domain configuration: Step 1: Create a domain

- Create a domain

```
idg # configure terminal

idg(config)# domain mydomain
idg(config domain mydomain)# summary "test domain for user"
idg(config domain mydomain)# visible-domain default
idg(config domain mydomain)# exit
```

Figure 5-24. User and domain configuration: Step 1: Create a domain

These sets of commands create a user account that is restricted to a specific domain. Currently, this user account cannot log on to the CLI. As an exercise, change the user account configuration to use the CLI.

### Example

Create a domain that is called `mydomain` that allows read-only access to the default domain.

## User and domain configuration: Step 2: Create a user group

- Create a user group

```
idg(config)# usergroup developer_test_user
idg(config usergroup developer_test_user)# summary "test user group"
idg(config usergroup developer_test_user)# access-policy
 /default/?Access=r"
idg(config usergroup developer_test_user)# access-policy
 /mydomain/?Access=r+w+a+d+x+
idg(config usergroup developer_test_user)# exit
```

Figure 5-25. User and domain configuration: Step 2: Create a user group

---

### 1+1=2 Example

Create a user group that is called `developer_test_user` that defines two access policies:

The access-policy string `"/default/*?Access=r"` allows read access to the default domain.

The access-policy string `"/mydomain/*?Access=r+w+a+d+x+"` restricts access to the `mydomain` domain.

---

## User and domain configuration: Step 3: Create a user

- Create a user

```
idg(config)# user test_user
New User configuration
idg(config user test_user)# access-level group-defined
idg(config user test_user)# group developer_test_user
idg(config user test_user)# password passw0rd
Re-enter new password: *****
idg(config user test_user)# exit
```

Figure 5-26. User and domain configuration: Step 3: Create a user

1+1=2

### Example

Create a user account `test_user`, whose privileges are defined in the `developer_test_user` user group.



## Configuration files

- On startup, each domain runs CLI commands to create objects within the domain
  - CLI commands are contained in an ASCII file on the encrypted RAM file system of the appliance
  - Default domain: **autoconfig.cfg**
  - Non-default domains: **<domain>.cfg**
- Resources that are created by using the Web or the XML Management Interface are converted into the corresponding CLI commands

The screenshot shows a user interface for managing XML configurations. On the left, there's a navigation bar with 'Domain: default ▾' and a 'Save Configuration' button, which is highlighted with a red box. To its right are 'Logout' and the 'IBM.' logo. To the right of the interface is a command-line window showing the following text:

```

configure terminal
...
xmlfirewall 'simpleFirewall'
 local-address 0.0.0.0 2092
 remote-address 127.0.0.1 1001
 stylesheet-policy simpleFirewall
 response-type unprocessed
exit

```

Below the interface, the text 'Using CLI and the XML Management Interface to configure appliance access' is visible. At the bottom right, it says '© Copyright IBM Corporation 2018'.

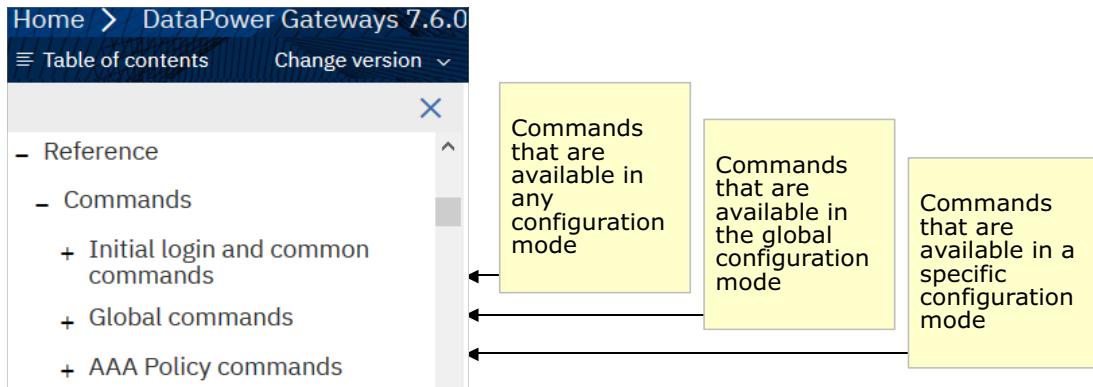
Figure 5-27. Configuration files

This configuration file shows the creation of a simple XML firewall service.

The default domain uses an `autoconfig.cfg` file, which contains the commands to create and configure Ethernet interfaces, domains, user groups, user accounts, and more. When the appliance starts, this file is initially run to create the respective objects.

## CLI commands in the information center

CLI commands are documented in the **Command** subsection of an appliance's **Reference** section.



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-28. CLI commands in the information center*

For more information on CLI commands, see

[https://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0/com.ibm.dp.doc/readingsyntaxstatements.html](https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/readingsyntaxstatements.html)

## Administration by using the XML Management Interface (XMI)

- XMI supports various endpoints for different protocols and tools that can perform administrative tasks
- To use XMI:
  - Enable the service, which is disabled by default
  - Select the appropriate endpoints to support
  - Ensure that the requests use the correct URI for the endpoint

[Using CLI and the XML Management Interface to configure appliance access](#)

© Copyright IBM Corporation 2018

*Figure 5-29. Administration by using the XML Management Interface (XMI)*

The DataPower Gateway can be configured and managed completely through the XML management interface. When enabled, this interface allows you to send status and configuration requests to the DataPower Gateway.

## WebGUI setup of the XML Management Interface

Select Network > Management > XML Management Interface

- **Local IP address** is the Ethernet interface where the service listens for requests
- The default port is 5550
- Default selections are:
  - SOAP Management URI
  - SOAP Configuration Management
  - SOAP Configuration Management (v2004)
  - AMP Endpoint
  - SLM Endpoint

For CLI, there is an **xml-mgmt** command to configure the support.

Administrative State	
<input checked="" type="radio"/> enabled	<input type="radio"/> disabled
Local address	172.16.78.47
Port Number	5550 *
Access Control List	xml-mgmt
Comments	
Enabled Services	<input type="checkbox"/> SOAP Management URI <input checked="" type="checkbox"/> SOAP Configuration Management <input type="checkbox"/> SOAP Configuration Management (v2004) <input checked="" type="checkbox"/> AMP Endpoint <input checked="" type="checkbox"/> SLM Endpoint <input checked="" type="checkbox"/> WS-Management Endpoint <input checked="" type="checkbox"/> WSDM Endpoint <input type="checkbox"/> UDDI Subscription <input checked="" type="checkbox"/> WSRR Subscription

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-30. WebGUI setup of the XML Management Interface

Enable the XML Management interface interface and note the port number that is used for communication. The typical value is 5550.

Admin access is required to enable this interface. The local IP address of 0.0.0.0 means that the appliance listens for requests on all of the IP addresses of the appliance. A security good practice is to restrict access to the XML management interface based on the appliance Ethernet interfaces. Enter the IP address of the management interface in the local address field to allow access by using that IP address.

The service level monitoring (SLM) policy peer sharing uses SOAP to communicate between appliances.

The Access Control List is a DataPower object that lists one or more IP address ranges that can be allowed to use the XML Management Interface, or denied access.

The recommendation is to **disable** “SOAP Management URI”. With this setting enabled, valid messages that are sent by using the SOAP Configuration Management or AMP format are compared to the older SOAP Configuration Management V2004 format and marked as invalid.

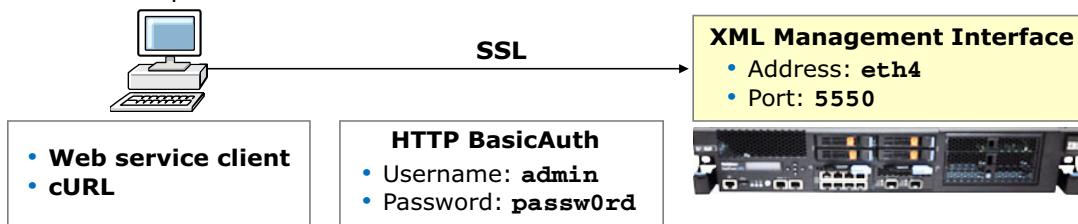
## Administration by using SOAP

Common approaches to manage the appliances and configuration use SOAP:

- XML Management Interface
- Appliance Management Protocol (AMP)

The SOAP interface provides advantages over other approaches:

- Programmatic: Build your own custom management application by using a programming language like Java (WAMT)
- Run remotely without any tools
  - WebGUI requires a web browser
  - CLI requires an SSH client



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-31. Administration by using SOAP

The SOAP configuration management endpoint in the XML management interface was also known as “SOMA” (SOAP management). This term is used as a parameter in the CLI.

WebSphere Appliance Management Toolkit is a Java and Jython toolkit that can be used to create batch or GUI-based classes to send AMP-related SOAP messages.



## Communicating with the XML Management Interface

- SSL communication is required to use the XML Management Interface:
  - Uses the factory-shipped DataPower certificate
  - You can deploy a custom SSL profile with your own certificate and key



- SOAP request is sent over HTTPS (HTTP + SSL)
  - Request must use the HTTP POST method
  - Must contain a **BasicAuth** HTTP header with the user name and password of an administrator account

Using CLI and the XML Management Interface to configure appliance access

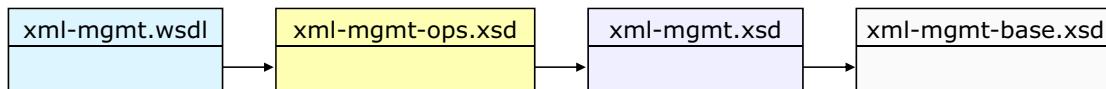
© Copyright IBM Corporation 2018

*Figure 5-32. Communicating with the XML Management Interface*

The SLM tab on the XML Management Interface page allows you to specify the update interval.

## SOAP Configuration Management (SOMA)

- The URI for the SOAP configuration management is:
  - `https:<ip-address>:<port>/service/mgmt/current`
- SOAP Configuration Management has a finer granularity than AMP, and provides more operations for manipulating configurations
- The DataPower appliance includes the following XML schema files, describing the allowed commands and data structures, which are stored in the `store:///` directory:
  - `xml-mgmt.wsdl`
  - `xml-mgmt-ops.xsd`
  - `xml-mgmt.xsd`
  - `xml-mgmt-base.xsd`



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-33. SOAP Configuration Management (SOMA)*

You might notice another set of WSDL or XSD files with the suffix 2004. These files represent an older schema and are provided for compatibility with releases before firmware V3.2.

Always retest your SOAP Configuration Management requests on every firmware release because the schema for SOAP Configuration Management is not assured to remain the same across versions.

## Sample SOMA request

- Example web service request for SOMA:

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
 xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
 <soapenv:Body>
 <dp:request
 xmlns:dp="http://www.datapower.com/schemas/management">

 <!-- Insert XML Management Interface requests here -->

 </dp:request>
 </soapenv:Body>
</soapenv:Envelope>
```

*Figure 5-34. Sample SOMA request*

The XML Management Interface request is a SOAP message, which requires an **Envelope** and **Body** tag. The SOAP header tag is optional. Tags between the Body tags are DataPower specific. Any commands that are submitted as SOMA requests are child tags of the `<dp:request>` tag.

The `<dp:request>` element contains an optional `domain` attribute to restrict the operation to the specified domain.

## Using cURL to issue the status request

```
C:>curl --data-binary @SOMAActiveUsers.xml
https://myDP.com:5550/service/mgmt/current
-u adminID:password -k
```

- Notice that:
  - The XML request is in SOMAActiveUsers.xml
  - The use of **https** because of the required SSL connection
  - The specific URI **service/mgmt/current** is used
  - An administrative ID and password are supplied by HTTP BasicAuth
  - The SSL server certificate is unconditionally accepted because of the **-k** parameter

Figure 5-35. Using cURL to issue the status request

## SOMA: Get status information

- Get a list of active users: <**dp:get-status**>

```

<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
 xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>

 <dp:request
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:get-status class="ActiveUsers">
 </dp:request>

 </env:Body>
</env:Envelope>

```

*Figure 5-36. SOMA: Get status information*

The `class` attribute is optional. However, not including it in a request returns all of the status information for the appliance. The `class` attribute specifies information about a specific object.

Other examples of allowed status class values are:

- CPUUsage
- EthernetInterfaceStatus
- MultiProtocolGatewaySummary
- ServicesStatus

## SOMA: Status information response (1 of 2)

- Response from <dp:get-status class="ActiveUsers">

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>
 <dp:response
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:timestamp>2012-08-15T11:49:40-05:00</dp:timestamp>
 <dp:status>
 <ActiveUsers
 xmlns:env="http://www.w3.org/2003/05/soap-
envelope">
 .
 .
 .
 </dp:status>
 </dp:response>
 </env:Body>
</env:Envelope>
```

Session ID	Domain	Name	Connection	IP address	Login
35	student01_domain	student01	web-mgmt	192.168.1.10	Mon Jul 26 12:33:40 2010

Figure 5-37. SOMA: Status information response (1 of 2)

The screen capture at the bottom of the figure is from the WebGUI, which is the same information that is returned in the SOAP response.

## SOMA: Status information response (2 of 2)

- Response from <dp:get-status class="ActiveUsers">

```

.
.
.

<session>81</session>
<name>admin</name>
<connection>web-gui</connection>
<address>1.2.3.4</address>
<login>Wed Aug 11 10:39:19 2012</login>
<domain>default</domain>
</ActiveUsers>
</dp:status>
</dp:response>
</env:Body>
</env:Envelope>

```

Session ID	Domain	Name	Connection	IP address	Login
35	student01_domain	student01	web-mgmt	192.168.1.10	Mon Jul 26 12:33:40 2010

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-38. SOMA: Status information response (2 of 2)

## Perform actions: Perform administrative actions

- Save the **default** domain configuration: <**dp:do-action**>

```
<env:Envelope
 xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>
 <dp:request
 xmlns:dp="http://www.datapower.com/schemas/management"
 domain="default">
 <dp:do-action>
 <SaveConfig/>
 </dp:do-action>
 </dp:request>
 </env:Body>
</env:Envelope>
```

Figure 5-39. Perform actions: Perform administrative actions

## SOMA: Create a configuration object

- Create an application domain: **<dp:set-config>**

```
 . . .
<env:Body>
<dp:request
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:set-config>
 <Domain name="student01-domain">
 <UserSummary>
 Test domain for student account 01.
 </UserSummary>
 <NeighborDomain class="domain">
 default
 </NeighborDomain>
 </Domain>
 </dp:set-config>
</dp:request>
</env:Body>
 . . .
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-40. SOMA: Create a configuration object

When you export an application domain configuration through the WebGUI, the XML file structure matches the elements within the `dp:request` element. That is, the XML Management Interface to the XML management system uses the same XML schema as the XML configuration files.

## SOMA: Domain creation response

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
 xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>

 <dp:response
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:timestamp>
 2017-08-15T15:22:04-05:00
 </dp:timestamp>
 <dp:result>
 OK
 </dp:result>
 </dp:response>

 </env:Body>
</env:Envelope>
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-41. SOMA: Domain creation response

Each set configuration call returns a result value. If the administration operation fails, an error message and code might be in the result field.

## SOMA: Delete configuration objects

- Delete **User**, **UserGroup**, and **Domain** objects: <**dp:del-config**>

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
 xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>
 <dp:request
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:del-config>
 <User name="newuser"/>
 <UserGroup name="TestGroup"/>
 <Domain name="TestDomain"/>
 </dp:del-config>
 </dp:request>
 </env:Body>
</env:Envelope>
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-42. SOMA: Delete configuration objects

When you delete configuration objects, the order is important. If you attempt to delete a configuration object that another active object references, the deletion request fails.

## SOMA: Modify configuration objects

- Modify **UserSummary** field: `<dp:modify-config>`

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>
 <dp:request
 xmlns:dp="http://www.datapower.com/schemas/management">
 <dp:modify-config>
 <User name="student">
 <UserSummary>
 Administrator account
 </UserSummary>
 </User>
 </dp:modify-config>
 </dp:request>
 </env:Body>
</env:Envelope>
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-43. SOMA: Modify configuration objects

Building the body of the `<dp:modify-config>` tag is nontrivial. You must examine the DataPower management XML schema files to determine the structure.

## Error handling

- Invalid web service requests to SOMA result in a SOAP fault
  - A SOAP fault contains generic error information, which is good for security but bad for debugging problems
- System logs do not show detailed information about SOMA errors
  - Invalid SOMA requests cause most errors
- Enable “internal logging” to get more detailed error messages in the log
  - **Troubleshooting > Logging > Set Log Level**

Figure 5-44. Error handling

The SOAP fault returns generic information about the error that was associated with the requests to prevent unauthorized users from learning inside information about the DataPower appliance.

You can obtain more log information by using the troubleshooting page. When setting the log level, you can enable the internal logging flag. It reveals more logging information that can aid in debugging SOAP issues.

## Appliance Management Protocol (AMP)

- Similar to SOAP Configuration Management, AMP also uses a SOAP message format
- Many operations can be started from either approach, but the message formats are not identical
- A WSDL and XSD are supplied in the firmware **store:///** directory to describe the supported operations:
  - app-mgmt-protocol-v3.wsdl
  - app-mgmt-protocol-v3.xsd
- The URI for the AMP endpoint
  - /service/mgmt/amp/3.0
- AMP is considered to be a more stable WSDL across firmware versions

Figure 5-45. Appliance Management Protocol (AMP)

The Appliance Management Protocol is another SOAP-style management interface mode.

## AMP request: Get domain list

```
C:>curl --data-binary @AMP_getdomainlist.xml
https://dpedu3.torolab.ibm.com:5550/service/mgmt/amp
/3.0
-u admin:wb540382 -k
```

- Notice that:
  - The XML request is in the AMP\_getdeviceinfo.xml file
  - The use of https because of the required SSL connection
  - The specific URI service/mgmt/amp/3.0 is used
  - An administrative ID and password are supplied by HTTP BasicAuth
  - The SSL server certificate is unconditionally accepted because of the -k parameter

Figure 5-46. AMP request: Get domain list

## AMP request: Get domain list request message

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
 xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Body>
 <dp:GetDomainListRequest
 xmlns:dp="http://www.datapower.com/schemas/appliance/
management/3.0"/>
</soapenv:Body>
</soapenv:Envelope>
```

Figure 5-47. AMP request: Get domain list request message

## AMP request: Get domain list response

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
 xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
<env:Body>
 <amp:GetDomainListResponse
 xmlns:amp="http://www.datapower.com/schemas/appliance/
management/3.0">
 <amp:Domain>default</amp:Domain>
 <amp:Domain>domain200</amp:Domain>
 <amp:Domain>student100</amp:Domain>
 <amp:Domain>student95</amp:Domain>
 <amp:Domain>student97_domain</amp:Domain>
 </amp:GetDomainListResponse>
</env:Body>
</env:Envelope>
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-48. AMP request: Get domain list response

## REST Management Interface

- When enabled, you can send requests to the REST management interface to supported service protocols to manage the appliance
- Provides access to the gateway status, configuration, and operations
- The URI structure of the REST-formatted request indicates the nature of the request
  - The JSON-formatted response indicates the disposition of the request
  - Some requests can use a JSON payload to supply the needed information for the request
- Uses the HTTP GET, POST, PUT, and DELETE HTTP methods
  - The methods that are available for a specific URI can be determined by using an HTTP OPTIONS method
- REST management requests can be sent by:
  - Browsers
  - **Curl** or similar program

Using CLI and the XML Management Interface to configure appliance  
access

© Copyright IBM Corporation 2018

Figure 5-49. REST Management Interface

## REST Management Interface

- Can be managed from
  - CLI:
    - **rest-mgmt** command
  - Web management:
    - **Network > Management > REST Management Interface**

- Enabled/disabled
- Listening IP address
- Listening port
  - Default is 5554
- Custom SSL connection profile is allowed

**REST Management Interface**

Status:	 up
<b>Main</b>	
Enable administrative state:	<input checked="" type="checkbox"/>
* Local address:	0.0.0.0
* Port Number:	5554
Custom SSL server type:	Server Profile
Custom SSL server profile:	
Access Control List:	rest-mgmt

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-50. REST Management Interface

## The REST high-level resources

- GET `https://DPgateway:5554/mgmt/`
  - Trailing slash (“/”) is required
- JSON response:

```
{
 "_links": {
 "self": {"href": "/mgmt/"},
 "config": {"href": "/mgmt/config/"},
 "domains": {"href": "/mgmt/domains/config/"},
 "status": {"href": "/mgmt/status/"},
 "actionqueue": {"href": "/mgmt/actionqueue/"},
 "filestore": {"href": "/mgmt/filestore/"},
 "metadata": {"href": "/mgmt/metadata/"},
 "types": {"href": "/mgmt/types/"}
 }
}
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-51. The REST high-level resources*

The presence or absence of the trailing slash (“/”) is important.

### 1+1=2 Example

`curl GET https://192.168.100.201:5554/mgmt/ -u admin:passw0rd -k`

**"self":{"href":"/mgmt/"}**

Self-reference

**"config":{"href":"/mgmt/config/"}**

Entrance point for configuration operations (read, create, update, delete)

Typical URI structure:

`/mgmt./config/{domain_name}/{class_name}/{object_name}/{property_name}`

**"domains":{"href":"/mgmt/domains/config/"}**

GET only URI to return a list of the currently-defined domains

**"status":{"href":"/mgmt/status/"}**

Entrance point for status provider information

Typical URI structure:

/mgmt./status/{domain\_name}/{class\_name}/{property\_name}

**"actionqueue": {"href": "/mgmt/actionqueue/"}**

Entrance point to gateway management operations

**"filestore": {"href": "/mgmt/filestore/"}**

Gateway point for file resources

Get directories in a domain, files within a directory, contents of a file

**"metadata": {"href": "/mgmt/metadata/"}**

The metadata for objects within a specific domain

Similar to information in the DataPower XSD and WSDL

Lists “fields” within an object definition

Can also get available operations within a specific domain

**"types": {"href": "/mgmt/types/"}**

GET definition of types

Definition of elements that are used in object definition

## Sample REST requests: status request

- GET  
`https://DPgateway:5554/mgmt/status/default/DateTimeStatus`
  - No trailing slash
- JSON response:

```
{
 "_links": {
 "self": {"href": "/mgmt/status/default/DateTimeStatus"},
 "doc": {"href": "/mgmt/docs/status/DateTimeStatus"}
 },
 "DateTimeStatus": {
 "time": "Wed Feb 14 17:06:34 2018",
 "timezone": "EST",
 "tzspec": "EST5EDT,M3.2.0/2:00,M11.1.0/2:00",
 "uptime2": "4 days 23:56:43",
 "bootuptime2": "4 days 23:57:06"
 }
}
```

Figure 5-52. Sample REST requests: status request

“default” in the URI path is the domain.

## Sample REST requests: get User configuration

GET `https://172.16.78.49:5554/mgmt/config/default/User`

- JSON response: List of defined user accounts

GET

`https://172.16.78.49:5554/mgmt/config/default/User/student95`

- JSON response:

```
{
 "_links": {
 "self": {"href": "/mgmt/config/default/User/student95"},
 "doc": {"href": "/mgmt/docs/config/User" },
 "User": {
 "name": "student95",
 "mAdminState": "enabled",
 "UserSummary": "Developer account on the student 95 domain.",
 "AccessLevel": "group-defined",
 "GroupName": {
 "value": "student95_developer_group",
 "href": "/mgmt/config/default/UserGroup/student95_developer_group" }
 }
}
```

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-53. Sample REST requests: get User configuration

### 1+1=2 Example

---

`curl https://192.168.100.201:5554/mgmt./config/default/User -u admin:passw0rd -k`

---

## Sample REST requests: create a User

- POST `https://172.16.78.49:5554/mgmt/config/default/User`
- JSON request payload:

```
{
 "User": {
 "name": "studentXX",
 "Password": "studentXXpassword",
 "UserSummary": "Developer account in the student XX domain.",
 "AccessLevel": "group-defined",
 "GroupName": "studentXX_developer_group"
 }
}
```

- Response:
- HTTP status code: 201
- JSON response payload:

```
{
 "_links": {
 "self": {"href": "/mgmt/config/default/User"},
 "doc": {"href": "/mgmt/docs/config/User"},
 "location": {"href": "/mgmt/config/default/User/studentXX"}
 },
 "studentXX": "Configuration was created."
}
```

*Figure 5-54. Sample REST requests: create a User*

“default” in the URI path is the domain.

The request elements are similar to what is used for a SOMA request:

```
<User name="studentXX">
<Password>studentXXpassword</Password>
<GroupName>developer_studentXX_domain</GroupName>
<AccessLevel>group-defined</AccessLevel>
<UserSummary>Developer account in the student XX domain.</UserSummary>
</User>
```

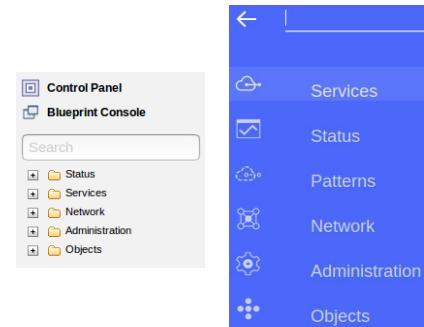
## Administration by using the web management interface

- The WebGUI and Blueprint Console provide most of the same administrative operations as CLI, XMI, and RMI
- Advantages
  - Available operations are visible in the navigation bar and menus
  - Fields and lists are used for parameters
  - Online help
  - Easy to view the system log for results or error messages
  - Easier to use for a novice, or for a user who performs administrative and development activities
- Disadvantages
  - Requires user interaction
  - Difficult to document what is to be or was performed
  - Cannot be automated
  - Might be difficult to use when network or appliance performance problems are occurring

Figure 5-55. Administration by using the web management interface

## The web interface navigation bar

- The links for administrative tasks are located under numerous sections in the navigation bar
- Status
  - Get the status of resources
- Network
  - Configure network resources
  - Enable management interfaces
- Administration
  - Manage domains, users, and user groups
  - Configure RBM settings
  - Configure the appliance settings
  - Configure the logging system



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

*Figure 5-56. The web interface navigation bar*

The Blueprint Console is the only web interface that contains an interface to Patterns.

## Unit summary

- Compare and contrast the DataPower management approaches: CLI, XML Management Interface, and the WebGUI
- Use CLI to configure domains, user groups, and users
- Configure administrative and development access to the appliance and resources
- Issue CLI commands to define and manage network resources
- Construct SOAP configuration management (SOMA) requests
- Use SOMA requests to configure resources and perform management functions
- Construct Appliance Management Protocol (AMP) requests
- Use AMP requests to run management functions

Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-57. Unit summary

## Review questions

1. **True or False:** Only users with **privileged** access are allowed access to the CLI interface.
2. **True or False:** Changes that are made by using the CLI are automatically persisted to disk. However, changes made by using the WebGUI are only persisted when the user clicks **Save Config**.
3. **True or False:** You must set up an SSL profile to communicate with the XML Management Interface service.
4. Which SOMA request tag would be used to create a configuration object?
  - A. `<dp:set-config class="domain" name="student" />`
  - B. `<dp:set-config>  
 <domain>student</domain>  
</dp:set-config>`
  - C. `<dp:update-config class="domain" name="student"/>`
  - D. `<dp:create-config>  
 <domain>student</domain>  
</dp:create-config>`

Using CLI and the XML Management Interface to configure appliance  
access

© Copyright IBM Corporation 2018

Figure 5-58. Review questions

Write your answers here:

- 1.
- 2.
- 3.

## Review answers

1. **False.** CLI access can be assigned through the user group CLI commands.
2. **False.** Use the `write mem` CLI command to persist changes to the appliance flash memory.
3. **False.** The XML Management Interface service is preconfigured with an SSL proxy profile that uses the factory installed DataPower certificate. You can create your own custom SSL proxy profile.
4. **B.** The second SOMA request would be used:

**B. <dp:set-config>**  
**<domain>student</domain>**  
**</dp:set-config>**

Figure 5-59. Review answers

## Exercise 2

- Using the CLI and the XML Management Interface to manage DataPower appliances

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Figure 5-60. Exercise 2

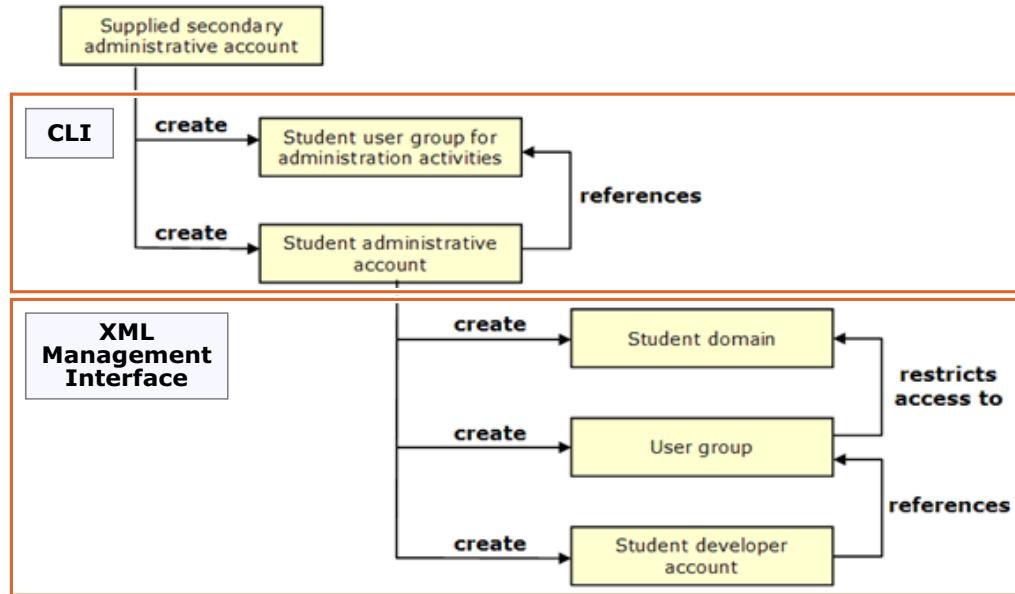
## Exercise objectives

After completing this exercise, you should be able to:

- Create DataPower resources by using the CLI
- Create DataPower resources by using SOMA requests
- Send appliance management requests by using AMP

*Figure 5-61. Exercise objectives*

## Exercise overview (1 of 3)



Using CLI and the XML Management Interface to configure appliance access

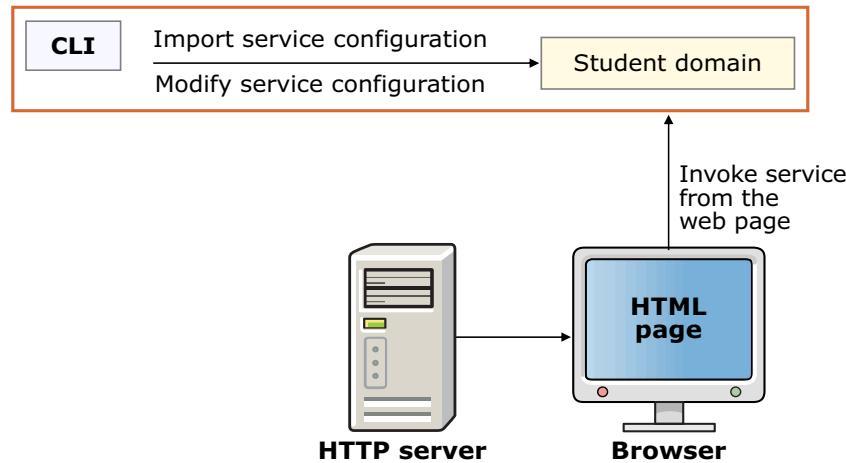
© Copyright IBM Corporation 2018

Figure 5-62. Exercise overview (1 of 3)

First, using command-line interface CLI commands, you create your administrative user account and administrative user group.

Using the administrative account, XML Management Interface requests are used to create the developer domain, user group, and account.

## Exercise overview (2 of 3)



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

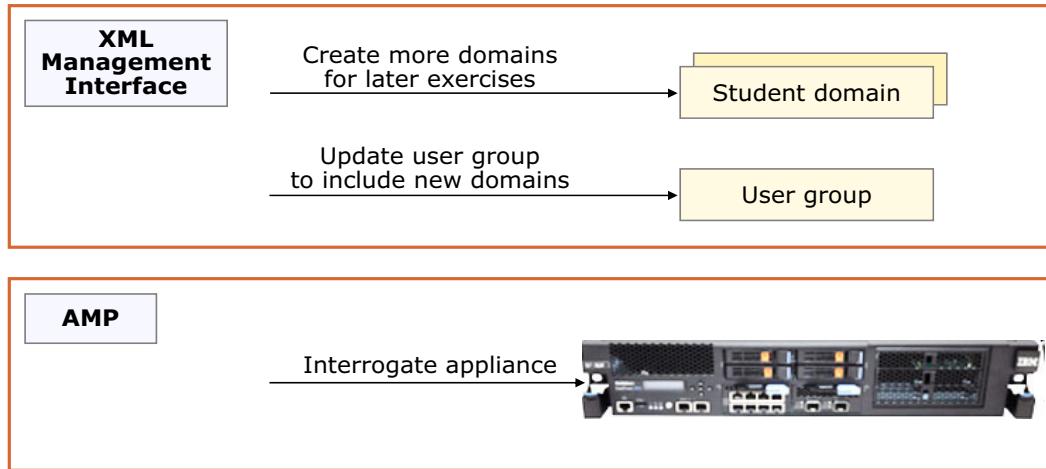
Figure 5-63. Exercise overview (2 of 3)

CLI commands are used to retrieve an exported service configuration from an HTTP server and import it into the developer domain. The service is a multi-protocol gateway that issues SOMA requests to an appliance.

Because the service has a generic port assignment, CLI commands are used to update the port to the student-specific number.

The service is tested by requesting a page from the HTTP server. After entering data into the page, the page invokes the multi-protocol gateway.

## Exercise overview (3 of 3)



Using CLI and the XML Management Interface to configure appliance access

© Copyright IBM Corporation 2018

Figure 5-64. Exercise overview (3 of 3)

XML Management Interface requests are issued to create domains that are needed in later exercises, and to update the developer user group to include the new domains.

Finally, AMP requests are sent to the appliance to determine different states.

---

# Unit 6. DataPower services overview

## Estimated time

00:30

## Overview

This unit describes the service types that are supported on the DataPower gateway. You examine, at a high level, what a service is and what it can communicate with. You also review the characteristics of each service type, and examine the relationships between the XML-based services.

## How you will check your progress

- Review questions

## References

IBM DataPower Gateways 7.6.0 Knowledge Center:

[http://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0](http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0)

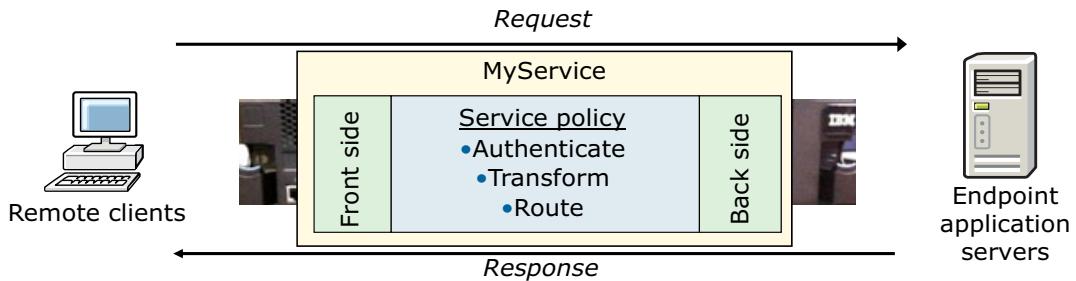
## Unit objectives

- Define what a DataPower service is
- List the supported services on the DataPower gateway
- Describe the similarities and differences in the features that each DataPower service supports

*Figure 6-1. Unit objectives*

## Services in a DataPower gateway

- A service on the gateway is required to deliver DataPower functions
- A gateway supports one or more configured services



- A service is of a specific type
- The type that is selected depends on:
  - Processing needs
  - Communication protocol
  - Type of endpoint application servers

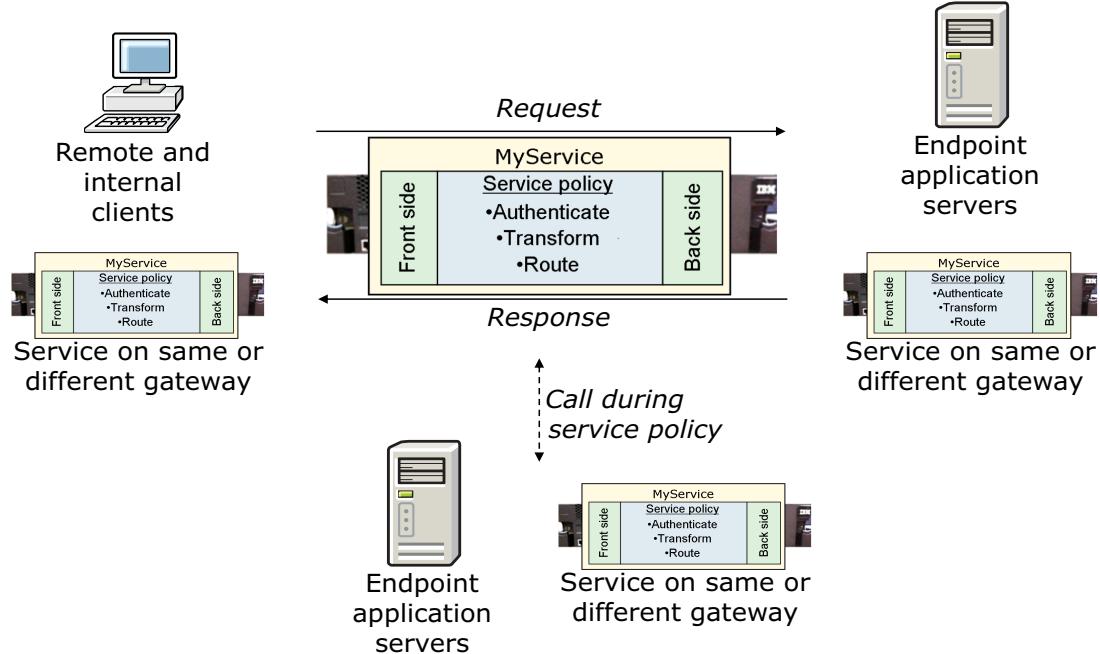
[DataPower services overview](#)

© Copyright IBM Corporation 2018

Figure 6-2. Services in a DataPower gateway

A service is composed of front side specifications, a service policy, and back-side specifications.

## Front sides and back sides, and sideways



DataPower services overview

© Copyright IBM Corporation 2018

Figure 6-3. Front sides and back sides, and sideways

The front side of a service can receive requests from a remote client, an internal client, or another service on the appliance.

The terms “front side” and “back side” are relative terms.

The “front side” listens for messages from clients or other DataPower services. The clients can be internal, remote, or even on the cloud.

While executing a service policy, the service can make a call to other services on the appliance or to other application servers.

The back side of the service calls the target application server, or perhaps another service on the appliance.

The “back side” sends the potentially modified client message to an application server or perhaps another DataPower service.

## Services available on the DataPower gateway

- XML firewall
  - Secures and offloads XML/JSON processing from back-end XML/REST-based applications that use HTTP/HTTPS
  - Supports XML/JSON encryption and signatures, AAA, routing, XML/JSON schema validation, more
- Multi-protocol gateway (MPGW)
  - Enhancement of XML firewall to support multiple protocols at the same time
- Web service proxy (WS-Proxy)
  - Enhancement of XML firewall to support WSDL-based configuration
  - Virtualizes and secures back-end web service applications
- B2B Gateway
  - Supports specialized B2B message traffic between partners
- Access Manager Reverse Proxy
  - Secure web access to unified (junctioned) web servers
  - Integrates with IBM Security Access Manager
- Web application firewall (WAFW)
  - Secures and offloads processing from web-based applications
  - Threat mediation, AAA, and web-based validation

[DataPower services overview](#)

© Copyright IBM Corporation 2018

Figure 6-4. Services available on the DataPower gateway

List the supported services and high-level features of each service.

AAA stands for *authentication, authorization, and auditing*.

The primary DataPower services are the multi-protocol gateway and the web service proxy.

The web service proxy configuration is WSDL-based. It is the only service that *requires* a WSDL file.

All services support monitors and logging.

## XML firewall service

- Secure and offload processing from back-end XML-based applications with the XML firewall service
  - Validates the schema of the message
  - Ensures document legitimacy by providing tamper protection with XML signatures
  - Protects against XML-based attacks
  - Uses XML encryption to secure messages
  - Provides dynamic routing of XML documents to the appropriate back-end service
  - Access control is based on user credentials in the message
  - Most functions are available for REST/JSON
- Available on the XG45, XI52, IBM DataPower Gateway



Figure 6-5. XML firewall service

The features that are listed for the XML firewall are not exhaustive. The XML firewall also supports the same features as the XSL proxy.

An XML firewall uses a document processing policy to enforce the features that are mentioned in the figure. For example, a firewall policy can require that messages be decrypted and then schema-validated. Other features, such as XML signatures, access control, and dynamic routing, have associated actions that are used in a firewall policy.

XML threat protection and SSL communication are configured at the service level instead of the policy level.

## Multi-protocol gateway service

- A multi-protocol gateway (MPGW) connects client requests that are sent over one or more transport protocols to a back-end service that uses the same or a different protocol
  - Single policy that is applied to multiple messages over many protocols
  - Uses static or dynamic back-end protocol and URL
- Features are a *superset* of the XML firewall
- Preferred choice for non-WSDL-based services
- Available on the XG45, XI52, XB62, IBM DataPower Gateway

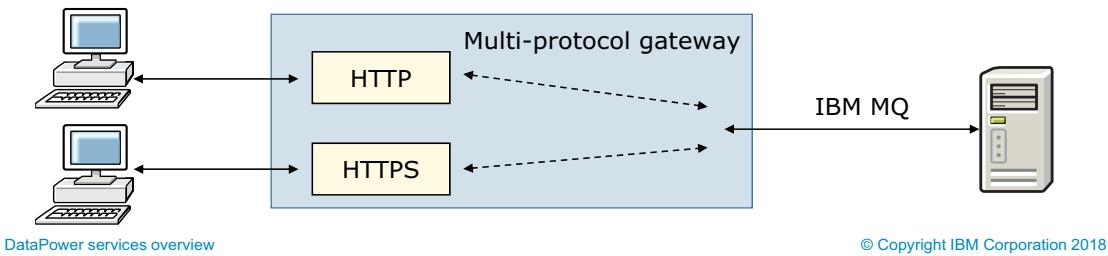


Figure 6-6. Multi-protocol gateway service

The multi-protocol gateway does not support the loopback proxy mode as supported by the XML firewall and XSL proxy, but the same effect can be specified by using a DataPower variable within the service.

The protocol that is used on the client-side of the gateway does not need to be the same as the one on the back end.

The supported protocols are HTTP, HTTPS, FTP, FTPS, SFTP, NFS, raw XML, WebSphere MQ, WebSphere MQ File Transfer Edition (MQFTE), TIBCO EMS, WebSphere JMS, and IMS Connect.

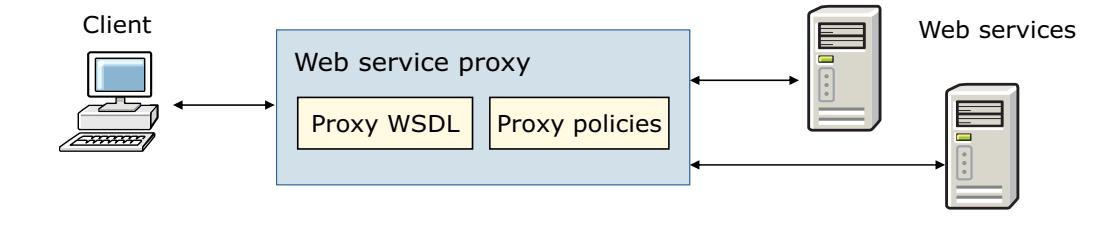
The gateway can use GET and PUT queues to communicate by using WebSphere MQ messages.

HTTP, HTTPS, and raw XML listen on specific IP addresses and ports. WebSphere MQ polls for requests from a WebSphere MQ queue manager.

FTP and NFS poll for messages from their respective servers.

## Web service proxy service

- The web service proxy (WS-Proxy) is used to secure and virtualize multiple back-end web service applications
  - WSDL-based configuration
  - Policies, monitoring, and logging can be done at various levels of the WSDL file
  - WSDL and governance policy can be updated dynamically
- Features are a *superset* of the XML firewall
- Preferred* choice for WSDL-based services
- Available on the XG45, XI52, XB62, IBM DataPower Gateway



DataPower services overview

© Copyright IBM Corporation 2018

Figure 6-7. Web service proxy service

An XML firewall or multi-protocol gateway can be created from a WSDL file as well. However, the web service proxy is simpler to configure with the WSDL file because it includes built-in support for creating rules at different levels of the WSDL, and service virtualization.

Multiple WSDL files can be associated with the web service proxy, producing a single virtual WSDL that the client sees.

The web service proxy does not support the loopback proxy mode as supported by the XML firewall and XSL proxy, but the same effect can be specified by using a DataPower variable within the service.

You can receive requests over various transports (front side handlers). It is the same list that a multi-protocol gateway supports for the front side.

A company might have multiple web services that it wants to expose. Using a WSDL file, the administrator can choose web services, and specific operations in each web service, to expose to clients. Clients see this new “service” and operations as if they were running on the appliance, and are unaware of the actual endpoints involved.

## B2B gateway service

- Supports common B2B protocols
  - AS1, AS2, AS3, ebMS
- Handles different message body contents
  - XML, EDI ANSI X12, EDIFACT, Binary (non-XML, non-EDI)
- AS2 and AS3 packaging or unpackaging
- EDI, XML, and binary payload routing
- Works with B2B Partner Profiles that supports multiple destinations
- Non-repudiation of origin and receipt of all AS2 and AS3 messages
- Encrypted on-gateway document storage, metadata storage, B2B state management
- Requires the B2B feature



B2B Gateway Service

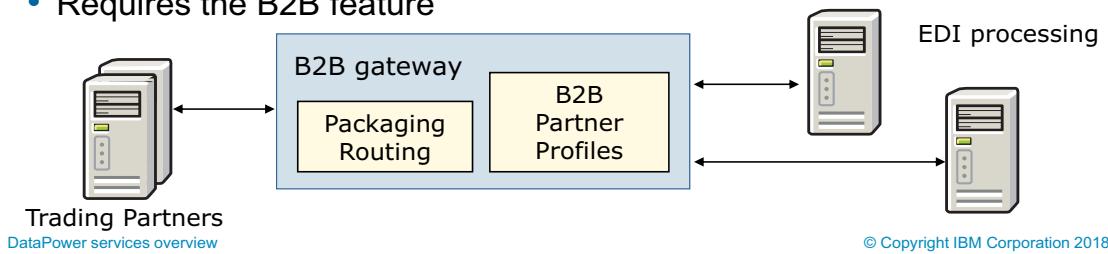
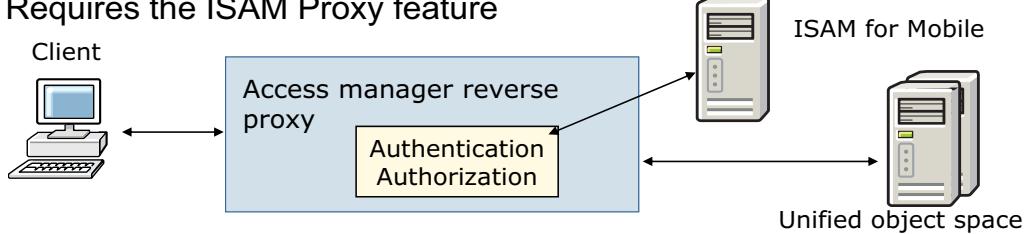


Figure 6-8. B2B gateway service

The B2B feature is included on the XB62.

## Access manager reverse proxy

- Secures HTTP/HTTPS access to protected web resources
- Provides a unified object space of protected resources through a “junction” technology
- Integrates with IBM Security Access Manager (ISAM) for Web
  - Authentication, authorization, session management
- Integrates with ISAM for Mobile for advance access management use cases
  - One time password, multi-factor authentication, context-based access
- Can “chain” to other DataPower services so they can provide further message mediation
- Requires the ISAM Proxy feature



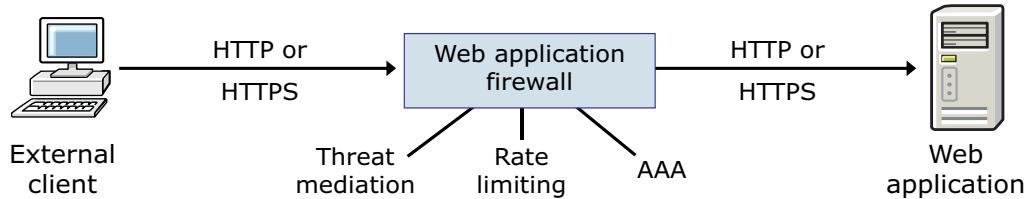
DataPower services overview

© Copyright IBM Corporation 2018

Figure 6-9. Access manager reverse proxy

## Web application firewall service

- A web application firewall (WAFW) is used to secure and offload processing from web-based applications
  - Proxies back-end web applications by listening for requests on multiple Ethernet interfaces and TCP ports
  - Provides threat mediation, AAA, and SSL
  - Limits the number of requests or simultaneous connections to back-end web applications
  - Configuration steps are different from MPGW and WS-Proxy
- Customized firewall for HTTP-based traffic
- Available on the XG45, XI52, XB62, IBM DataPower Gateway



DataPower services overview

© Copyright IBM Corporation 2018

*Figure 6-10. Web application firewall service*

## Other services

- Web token service
  - Loopback service to support OAuth token services
- Interoperability test service
  - Development tool that simplifies the testing of stylesheets and schemas
- XSL proxy
  - Accelerates XML processing, such as schema validation and XSL transformations
  - One of original DataPower service types (deprecated)
- XSL coprocessor service
  - Loopback service that accepts JAXP-based requests
  - One of original DataPower service types (deprecated)
- Four secondary services are available for handling message traffic without running a service policy
  - HTTP service: Serves documents from a gateway directory
  - TCP proxy service: Forwards TCP traffic to another address and port
  - SSL proxy service: Used by log targets to securely connect to remote log systems
  - Cloud Gateway Service: Creates a Cloud Gateway service, which can be used with IBM Cloud Cloud Integration

Figure 6-11. Other services

XSL coprocessor service is a variant of the XSL proxy service. It is deprecated, and should not be used. In the past, this service was commonly used to test style sheets. This capability is now available in the interoperability test service. Although this service supported JAXP-based requests, there is no Java running in the firmware. It just conforms to the JAXP interface.

## Which service type should you use?

- If you are WSDL and web services-focused, choose the **web service proxy**
  - Present a single virtual WSDL to the clients that is composed of multiple WSDLs on the back end
  - Require different processing for the individual operations in the WSDLs
- If you are processing B2B messages with your trading partners, choose the **B2B gateway**
- If you require sophisticated authorization of clients by ISAM for protected web resources, select the **access manager reverse proxy**
- For general message processing/routing/authorization, select the **multi-protocol gateway**

Figure 6-12. Which service type should you use?

## Unit summary

- Define what a DataPower service is
- List the supported services on the DataPower gateway
- Describe the similarities and differences in the features that each DataPower service supports

Figure 6-13. Unit summary

## Review questions



1. True or False: The web service proxy is the only service that requires a WSDL.
2. True or False: While running a service policy, the service can invoke only other services on the gateway.
3. Which service type is the best choice for this requirement? A service needs to schema-validate and transform a message before it is placed on a IBM MQ queue for mainframe processing. Input comes over HTTPS from external clients, and over HTTP from internal clients.
  - A. XML firewall
  - B. Multi-protocol gateway
  - C. Web service proxy
4. Which service type is the best choice for this requirement? An enterprise has operations within several existing web services that it wants to expose to external clients as a single web service.
  - A. XML firewall
  - B. Multi-protocol gateway
  - C. Web service proxy

DataPower services overview

© Copyright IBM Corporation 2018

*Figure 6-14. Review questions*

Write your answers here:

- 1.
- 2.
- 3.

## Review answers (1 of 2)

1. True or False: The web service proxy is the only service that requires a WSDL.  
The answer is True.
2. True or False: While running a service policy, the service can invoke only other services on the gateway.  
The answer is False. While running a service policy, the service can invoke other application servers and other services on the gateway.
3. Which service type is the best choice for this requirement? A service needs to schema-validate and transform a message before it is placed on a IBM MQ queue for mainframe processing. Input comes over HTTPS from external clients, and over HTTP from internal clients.
  - A. XML firewall
  - B. Multi-protocol gateway
  - C. Web service proxyThe answer is B. This service type can support both an HTTP and an HTTPS front side handler, and can communicate with a IBM MQ queue on the back side.



Figure 6-15. Review answers (1 of 2)

## Review answers (2 of 2)

4. Which service type is the best choice for this requirement?

An enterprise has operations within several existing web services that it wants to expose to external clients as a single web service.

- A. XML firewall
- B. Multi-protocol gateway
- C. Web service proxy

The answer is C. This service type can present a single virtual web service to the client that is composed of specific operations from several web services.



Figure 6-16. Review answers (2 of 2)

---

# Unit 7. Using the Web Management Blueprint Console to configure appliance

## Estimated time

00:30

## Overview

This unit shows you how to create new user accounts, user groups, and domains. You also learn how to obtain domain configuration from external resources and manage domain resources remotely. The unit describes the Blueprint Console approach to resource definition, and explains how to complete Web Management authentication by using external Directory Services such as LDAP.

## How you will check your progress

- Review questions

## Unit objectives

- Use the Web Management Blueprint Console to create user accounts, user groups, and domains
- Use the role-based management (RBM) policy builder to restrict access to objects within a domain
- Use the Blueprint Console to configure authentication with the Lightweight Directory Access Protocol (LDAP)

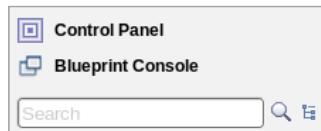
Using the Web Management Blueprint Console to configure appliance  
access

© Copyright IBM Corporation 2018

*Figure 7-1. Unit objectives*

## Getting to the Blueprint Console

- Two ways to get to the Blueprint Console:
  - Its own URL:  
`https://<appliance_address>:<WebGUI_port>/dp`
  - Click **Blueprint Console** from the WebGUI:



- It opens a second browser tab or browser window
  - Shared session between Blueprint Console and WebGUI, so the WebGUI login and timeout applies to both
  - Blueprint Console has its own Login page where you can log in when a WebGUI timeout occurs

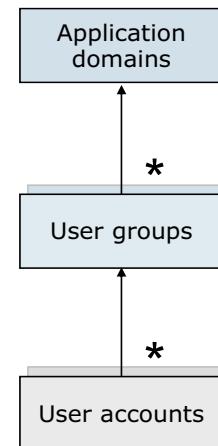
Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-2. Getting to the Blueprint Console

## Administrative access control

- **Application domains** provide a virtualized, enclosed environment for services
  - Only the **default** domain allows administrators to do system-level tasks, such as configuring an Ethernet interface
- **User groups** apply a specific access policy to a set of user accounts
  - **Privileged** access allows users to do system-level tasks
  - **User** access provides read-only guest access
  - **Group-defined** relies on a user-defined, fine-grained access policy for each resource
- **User accounts** provide users with access to the Web Management (WebGUI or Blueprint Console) service



[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

Figure 7-3. Administrative access control

Users can also view more than one application domain's `local:` directory by using the visible domain setting for application domains.

Privileged and user access levels represent the highest and lowest access levels on the DataPower SOA Appliance. An administrator can use the group-defined setting to fine-tune the access level within either end of the spectrum.

User accounts that are created through the Web Management interface apply to the interface (CLI) and XML management interface as well.

## Separate or grouped application domains

- Considerations:
  - Objects, files, and keystore shareability and reusability
  - The concept of the domain as a virtual sandbox for developers and testers
  - Permissions for administrators or developers can be assigned to one or more domains and protects from the accidental or malicious change of security policies
- Large monolithic applications are in their own separate domains
  - Smallest practical unit is a domain
- Smaller, related applications are aggregated into single domains
  - Resources are often shared between the various services
  - Enabling, disabling, and restarting a domain affects all the related services at the same time
- The **default** domain on the device contains the network configuration, log target, and management services
  - Create services in non-default domains so they can be separately managed, exported, and imported

[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

*Figure 7-4. Separate or grouped application domains*

The **default** domain on the device contains the network configuration, log target, and management services.

Do not define any services in the default domain.

Create services in non-default domains so they can be separately managed, exported, and imported.



## Create an application domain

The screenshot illustrates the process of creating an application domain in the Blueprint Console. It consists of two main parts: a left sidebar and a right configuration dialog.

**Left Sidebar (Administration View):**

- Step 1:** Click the **Administration** icon.
- Step 2:** In the **Configuration** section, click **Application Domain**.
- Step 3:** Click the **New...** button.

**Right Configuration Dialog (Create Application Domain Dialog):**

- Name:** (Mandatory field) (3)
- Comments:** (4)
- Visible application domains:** Set to **default** (5)
- Add** button (6)
- File permission to the local directory:** A list of checkboxes:
  - Allow files to be copied from
  - Allow files to be copied to
  - Allow files to be deleted
  - Allow file content to be displayed
  - Allow files to be run as scripts
  - Allow subdirectories to be created
- File-monitoring of the local directory:** A list of checkboxes:
  - Enable auditing
  - Enable logging
- Apply** and **Cancel** buttons (7)

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-5. Create an application domain

- From the Blueprint Console, click the **Administration** icon. Then, select **Configuration > Application Domain**.
- In the listing of available application domains (not shown), click **New**. Provide a name for the new application domain; this field is mandatory.
- Leave the **Enable administrative state** option as **selected**. The administrative state setting determines whether a particular DataPower object is available for use.
- Enter any appropriate comments.
- The visible domains setting determines whether this domain can access files in the **local:** file store of another application domain. In the figure, **student95** can access the files in the **local** file store of the **default** domain.
- Local file permissions determine the access rights to files stored in the local file store of the current domain.
- When enabled, changes to files in the local file store generate auditing or logging events.

You use the **Configuration** option (not shown) to specify whether the configuration is stored locally or is imported from a specified URL every time the configuration is saved or the system is restarted.

IBM Training IBM

## Configuration mode of an application

The **Configuration mode** specifies whether the configuration of the domain is:

- **Local**: Configuration file is on the appliance file system
- **Import**: Configuration file is on a remote web server
  - Import format is either ZIP or XML

**Configuration**

Configuration checkpoint limit:

Configuration mode:

**Apply** **Cancel**

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-6. Configuration mode of an application

When the configuration mode is specified as “Import from remote server”, two additional pop-ups are displayed:

Import URL specifies where the file is stored.

Import format:

- The ZIP import format includes the configuration and related files.
- The XML format contains just the configuration.

Remote configuration allows you to have multiple appliances retrieve the same version of the domain configuration.

The screenshot shows a web-based application titled "IBM Training" with the "IBM" logo in the top right corner. The main title is "View application domain status". Below it is a table titled "Application Domain" with the following columns: Name, Status, Op-State, Administrative state, Comments, Quiesce state, and Actions. The table lists five domains:

Name	Status	Op-State	Administrative state	Comments	Quiesce state	Actions
default	saved	up	enabled	Default System Domain		
FLYServices	saved	up	enabled			
student95_domain	saved	up	enabled	Test domain for student account 95.		
student95_import_domain	saved	up	enabled	Domain for student95_import_domain		
student95_remote_domain	saved	up	enabled	Domain for student95_remote_domain		

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-7. View application domain status

The application domain page lists all configured domains on the DataPower Gateway Appliance. This page is visible only from the default application domain.

## Configuration Checkpoints

- A Configuration Checkpoint contains configuration data for an application domain from a specific point in time
  - Saves the current state of the application domain without persisting it
  - An alternative to Save the configuration
  - Can be used for continuing work between sessions
- Saving Configuration Checkpoints
  - Select **Administration** then **Configuration > Configuration Checkpoints**
  - Enter the name and click **Save Checkpoint**

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

*Figure 7-8. Configuration Checkpoints*

Configuration checkpoints can also be used as a form of a rollback for a single domain.

Existing checkpoints can be removed, compared, or rolled back (that is, redefine the domain configuration).

The checkpoint file goes into the `chkpoint:` directory.

**User Group**  
student95\_developer\_group

Status: up

Name: student95\_developer\_group

Main

Enable administrative state: ⓘ

Access profile: ⓘ \* /student95\_domain/\*?Ao

Build ▾

Access Profile property syntax:  
address / domain / resource?Access=permissions& [field=value]

Editing Access profile property of User Group

Local address: ⓘ \*

Application domain: ⓘ student95\_domain

Resource type: ⓘ (all resources)

Local address match: ⓘ

Local port match: ⓘ

Directory match: ⓘ

File name match: ⓘ

Privileges: ⓘ

- Read
- Write
- Add
- Delete
- Execute

Figure 7-9. Manage user group details

User groups provide a convenient way for applying an access profile to a set of user accounts. The access profile policy syntax restricts the access permission of any user to which the user group is applied. If two access profile policies affect the same resource, the most specific policy is applied.

- **Address:** The DataPower SOA Appliance local IP address or local host alias.
- **Domain:** Specifies the name of one particular application domain. You can use a regex expression to indicate a group of domains.
- **Resource:** Represents one type of DataPower object within the configuration.
- **Permissions:** r (read), w (write), a (add), d (delete), or x (execute).
- **Field and value:** Specify a particular object, such as the name of a web service proxy.

In the figure, the users in the group are provided read access to all resources within the **student95** application domain.

Click **Build** to use a graphical form to build the access profile policy.



## Example: Access profile for the student admin group

- Student admin group has access to all resources in all domains, and read-only access to the store: directory and network settings

Status: ● up

* Name:	student95_admin_group
<b>Main</b>	
Enable administrative state:	<input checked="" type="checkbox"/>
Comments:	summary "student95 administrative user group"
Access profile:	<input type="text" value="/*/*?Access=rwadx"/> <span style="color: blue;">Build ▾</span> <input type="text" value="/*/file/store?Access=r"/> <span style="color: blue;">Build ▾</span> <input type="text" value="/*/network/interface?Access=r"/> <span style="color: blue;">Build ▾</span>

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-10. Example: Access profile for the student admin group

An access policy can use wildcard characters in regular expressions to define the same set of privileges to multiple resources.

IBM Training 

## Manage a user account

Status: up

\* Name: student95

**Main**

Enable administrative state:

Comments: Developer account on the student 95 domain.

Password:

\* Access level: Group defined

\* User group: student95\_developer\_group

Domain restriction (deprecated): No items.

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-11. Manage a user account

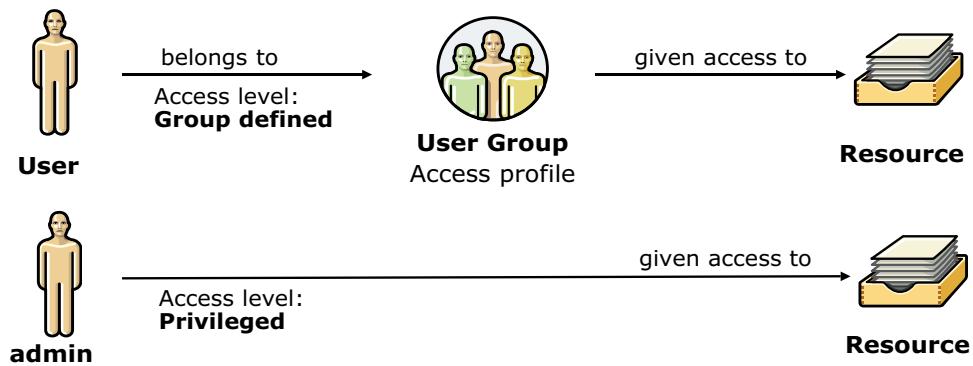
You can use the new user account dialog to create a user account and a user group at the same time. To access this dialog, click the **Administration icon**. Then, select **Access > User Account** from the navigation bar. On the User Account, click **New**.

The options on the access level drop down are: Group defined, Privileged, or User (deprecated). If Group Defined is selected, you are prompted to select the user group that the user belongs to.

The page shows the options for managing the student95 user account when the administrator is signed on to the Blueprint console.

## Role-base management (RBM)

- DataPower Gateway manages access through role-based management (RBM)
- RBM controls the relationships between authenticated users and resources
  - RBM policy determines whether to allow an **authenticated user** access to specific resources
  - RBM policy uses **access profiles** to determine **authorization** to resources



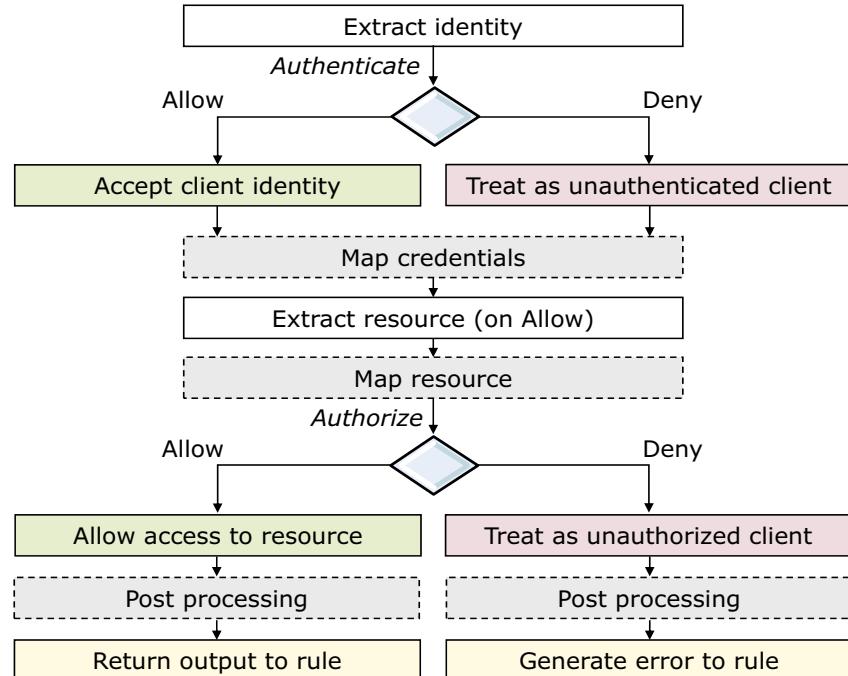
[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

Figure 7-12. Role-base management (RBM)

Role-based management provides a flexible and integrated way to control whether an authenticated user has the necessary permission to access resources through access policies.

## RBM policy processing



Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

Figure 7-13. RBM policy processing

The user logs in to the DataPower Gateway. The user is authenticated either by a remote authentication system or by the DataPower Gateway. The RBM policy determines whether to allow an authenticated user to access specific resources.

An AAA (authentication, authorization, audit) policy identifies a set of resources and procedures that determine whether a requesting client is granted access to a specific service, file, or document.

## Using RBM for the Web Management service

- Default access control to the Web Management service is managed through local DataPower objects
  - User, UserGroup, and Domain
- User access to domains and resources is controlled through the **UserGroup** object
  - Defines permissions for members of the group to resources in one or more domains
  - Permissions are defined by using an access profile string
  - Web Management access control can also use a remote authentication system, such as LDAP
  - Configure an RBM policy to enable access control off the box
  - Backup access policy can be defined when remote authentication is unavailable
- Be sure to add the **admin** user to the remote repository

[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

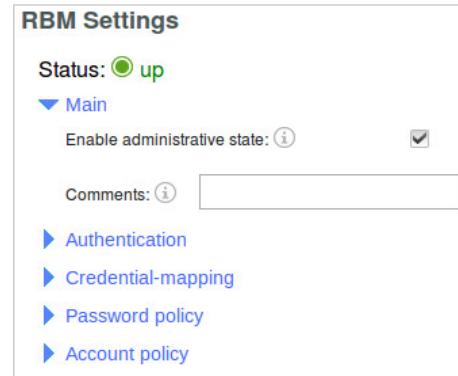
Figure 7-14. Using RBM for the Web Management service

Three types of user accounts exist: User, Group-Defined, and Privileged. The **User** and **Privileged** accounts do not use a user group object. They have a predefined access policy.

If you are using remote authentication for your users, be sure to add the **admin** user to the remote repository, or the **admin** user is locked out.

## Configure RBM authentication for WebGUI

- Configure an RBM object to manage access to the WebGUI
  - Select **Administration > Access > RBM Settings**
- A single object can be configured only in the **default** domain
  - The default access control method is **local user**
- When changes are applied, the changes take effect immediately
- An RBM policy can also be enforced over the CLI interface (enforce RBM on CLI)
  - Off by default
- Administrative login can be restricted to the serial port (Restrict admin to serial)
  - Off by default



Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

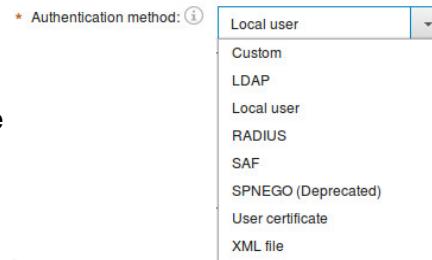
*Figure 7-15. Configure RBM authentication for WebGUI*

The user authentication method lists the methods for validating the identity of the user.

Based on the method that is selected, the page is updated with the relevant fields applicable for that method.

## RBM authentication methods

- **Custom:** Create an XSL stylesheet
- **LDAP:** Configure an LDAP server for authentication
- **Local user:** Uses DataPower objects (**User**, **UserGroup**, and **Domain**) to control access to the WebGUI
- **RADIUS:** Configure a RADIUS server
- **SAF:** Use z/OS NSS Server for SAF authentication
- **SPNEGO:** Configure a Kerberos keytab to decrypt the client Kerberos ticket
- **User certificate:** SSL User Certificate Authentication
- **XML file:** Create an RBM authentication file



Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

*Figure 7-16. RBM authentication methods*

Using the custom authentication method requires you to output an element that is named <OutputCredential> with the appropriate value that can be used in the authorization step.



## Configure LDAP RBM authentication method

Enter the information that is required to connect to an LDAP server for authentication:

- The **Local accounts for fallback** field defines backup users when the LDAP server is unavailable
  - Disabled (default)
  - All users
  - Specific users

Authentication	
Method	Authentication method: <b>LDAP</b>
* Server host:	<input type="text" value="172.16.78.222"/>
* Server port:	<input type="text" value="389"/>
LDAP version:	<input type="text" value="v2"/>
SSL proxy profile (deprecated):	<input type="text"/>
Load balancer group:	<input type="text"/>
Search LDAP for DN:	<input type="checkbox"/>
LDAP prefix:	<input text"="" type="text" value="cdc=ibm,dc=com"/>
LDAP read timeout:	<input type="text" value="60"/> Seconds

[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

Figure 7-17. Configure LDAP RBM authentication method

LDAP-based implementations require an X.500 DN (for example, `cn=Alice,dc=ibm,dc=com`) and a password. When configuring LDAP for authentication, it is typical to create a base DN (such as `dc=ibm,dc=com`) and then create one entry under this base for each user.

To make LDAP authentication more usable, RBM provides the LDAP suffix. Set the LDAP suffix to the base name under which user entries are found. Unless the LDAP suffix is an empty string, an X.500 compliant DN is built as follows:

- Prefix `cn=` to the user name.
- A comma precedes the value of the LDAP suffix.
  - For example, if the LDAP suffix is `dc=ibm,dc=com` and the user name is Alice, the DN is mapped as `cn=Alice,dc=ibm,dc=com`.
- The fallback user must also be defined within the remote authentication server and match the same credentials.
- Use the **Password Policy** tab to define a password policy.

## RBM authorization for the Web Management service

After authentication is complete, the authentication step emits a credential.

- Credential is mapped by using a user group, XML file, or custom method

Mapping credential methods:

- Local user group** maps the *credential* from the authentication step to the name of the **UserGroup** object
  - UserGroup** object defines permissions by using an access profile string
- XML file** uses an RBM policy file
  - Defines an access profile string that is based on the input credential
- Custom** uses an XSL stylesheet

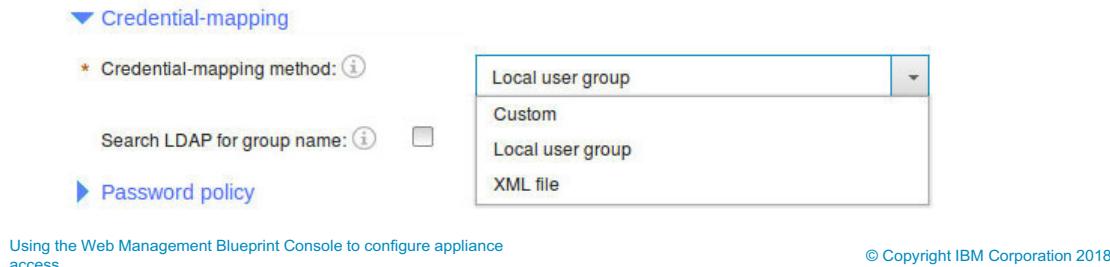


Figure 7-18. RBM authorization for the Web Management service

In the credential-mapping method, you set the method to map authenticated user credentials to the access profile.

When the Search LDAP for group name is enabled, the authenticated DN of the user and the LDAP search parameters are used as part of the LDAP search to retrieve all user groups that match the query. When a user belongs to multiple groups, the resultant access policy for this user is additive not most restrictive.

When LDAP authentication method is used, the Search LDAP for group name option must be selected to provide the credentials to map to the local user group for authorization.

The input credential in the XML file mapping credential method is obtained from the output of the authentication method.

For more information about the mapping credential methods that are supported for an authentication method, see the product documentation.

## XML file: RBM policy file for authorization

```

<?xml version="1.0" encoding="utf-8"?>
<AAAInfo xmlns="http://www.datapower.com/AAAInfo">
 <FormatVersion>1</FormatVersion>
 <Filename>store:///RMBMapping.xml</Filename>
 <Summary>RMB Mapping file</Summary>

 <MapCredentials>
 <InputCredential>admin</InputCredential>
 <OutputCredential>
 /*/*?Access=rwadx
 </OutputCredential>
 </MapCredentials>

 <MapCredentials>
 <InputCredential>myGroupAuth</InputCredential>
 <OutputCredential>
 /*/myDomain/*?Access=rwadx
 </OutputCredential>
 </MapCredentials>
</AAAInfo>

```

[Using the Web Management Blueprint Console to configure appliance access](#)

© Copyright IBM Corporation 2018

Figure 7-19. XML file: RBM policy file for authorization

This file is easily created by using the RBM policy file builder. An XML file can be defined for authentication, authorization, or both. Select **XML file** in the Mapping Credential method. Follow the prompts of the wizard to create a file.

This XML file defines two input credentials (`admin` and `myGroupAuth`). Any user authenticated is assigned one of these credential names. These names are associated to an output credential, which defines the permissions to access resources on the appliance.

## Unit summary

- Use the Web Management Blueprint Console to create user accounts, user groups, and domains
- Use the role-based management (RBM) policy builder to restrict access to objects within a domain
- Use the Blueprint Console to configure authentication with the Lightweight Directory Access Protocol (LDAP)

Using the Web Management Blueprint Console to configure appliance access

© Copyright IBM Corporation 2018

*Figure 7-20. Unit summary*

## Review questions

**1. True or False.** Domain configuration must be stored locally to enable service configuration.

**2. What is the syntax for the access profile string?**

- A. access/domain/  
resource?Address=permissions&[field=value]
- B. domain/address  
resource?Access=permissions&[field=value]
- C. address/domain/  
resource?Access=permissions&[field=value]

**3. True or False.** An LDAP server can be configured for Web Management user authentication, but a different authorization method can be used.

Figure 7-21. Review questions

Write your answers here:

- 1.
- 2.
- 3.

## Review answers

1. **False.** Domain configuration can be imported from an external URL.
2. **C.** What is the syntax for the access profile string?
  - A. access/domain/  
resource?Address=permissions&[field=value]
  - B. domain/address  
resource?Access=permissions&[field=value]
  - C.address/domain/  
resource?Access=permissions&[field=value]**
3. **True.** The Web Management service enables authentication by using LDAP. However, authorization is complete by mapping the authentication credentials to a local UserGroup object, by using an XML file, or a custom XSL stylesheet.

Figure 7-22. Review answers

# Unit 8. Troubleshooting

## Estimated time

00:45

## Overview

This unit describes the troubleshooting tools that are available for debugging problems on the DataPower gateway. Several tools are available for various problems, ranging from low-level networking tools to probes that aid in debugging service policies. The logging utilities are available for capturing information that the DataPower objects generate.

## How you will check your progress

- Review questions
- Lab exercise

## Unit objectives

- Identify the troubleshooting tools that are available on the DataPower appliance
- Capture information by using system logs for messages that pass through the DataPower gateway
- Configure the default system log for debugging
- Configure a multi-step probe to examine detailed information about actions within rules

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-1. Unit objectives

## Common problem determination tools

- Default system log
  - Displays system-wide log messages
  - Log messages can be filtered according to object and priority
- Audit log
  - Displays changes to the configuration of the gateway and files that are stored on the gateway
  - **Status > View Logs > Audit Log**
- Multi-step probe
  - Displays actions, messages, variable values as processing rule runs
  - Information is captured after processing rule runs
- Object status
  - Displays current operational status of all objects in the domain
  - **Status > Main > Object Status**
- Ping remote
  - Pings a remote host address to establish connectivity
- TCP connection test
  - Creates a TCP connection to remote destination to test connectivity
- Send test message
  - Builds and sends a SOAP request for testing
  - **Administration > Debug > Send a Test Message**

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-2. Common problem determination tools

## Gateway status information

- File system information
  - Displays available encrypted, temporary, space for file storage
  - **Status > System > Filesystem Information**
- CPU usage
  - Displays percentage of CPU usage
  - **Status > System > CPU Usage**
- System usage
  - Displays load and work queue status
  - **Status > System > System Usage**

Free Encrypted Space	13,052	Mbytes
Total Encrypted Space	14,896	Mbytes
Free Temporary Space	466	Mbytes
Total Temporary Space	512	Mbytes
Free Internal Space	971	Mbytes
Total Internal Space	1,024	Mbytes

10 sec	4	%
1 min	28	%
10 min	28	%
1 hour	28	%
1 day	28	%

Task ID	Task Name	Load (%)	Work List	CPU (%)	Memory (%)	File Count
1	main	1	0	2	1	258

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-3. Gateway status information

Unless otherwise noted, these screen captures are from the WebGUI. The Blueprint Console versions present the same information in a similar format.

It is a good practice to check the gateway file system memory for available space. The logging system can fill up the available file storage space, which can prevent the system from writing log entries. This situation prevents the system from processing messages.

**Temporary Space** is used for processing, logging, and debugging.

**Internal Space** is used for import, export, firmware upgrades, and debug data.

**System Usage** indicates the current load on the server and the length of the work queue. If the server suddenly slows down or becomes unresponsive, the cause might be system usage. If the system has a throttle in place, the high memory usage (load) might be causing the throttle to refuse connections.

## Troubleshooting

The Troubleshooting page contains the following tools:

- Ping Remote
  - Pings a remote host address
- TCP Connection Test
  - Creates a TCP connection to remote endpoint
- Packet Capture (default domain only)
  - Captures network packets to and from the gateway
- View System Log and generate log messages
  - Specifies log level of messages to record
  - Generates log messages for testing log targets
- Error Report
  - Includes the running configuration and relevant system log entries for errors
  - Emails error report to an email address
- XML File Capture (default domain only)
  - Captures inbound XML files that are submitted to the gateway
- Probe
  - Enables or disables probes on services



[Troubleshooting](#)

© Copyright IBM Corporation 2018

*Figure 8-4. Troubleshooting*

The best tool to use first when a problem occurs often depends on how the gateway is being used at the time.

During the development phase, the default system log is often the best place to start, followed by use of the multi-step probe.

During the testing phase, generating an error report (which contains the running configuration of the gateway and the relevant log entries) is an excellent first step, followed by use of the multi-step probe.

During the production phase, first check the system usage for load and work lists and then check the object status for objects that are changed to the down state. Finally, check the default system log.

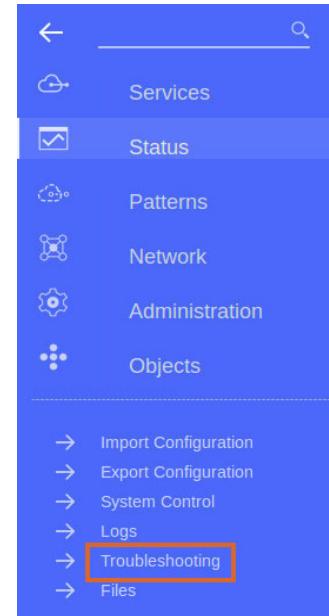
If you contact DataPower Support for a problem, you might need to include a generated error report.



## How to get to the Troubleshooting page

- WebGUI
  - Troubleshooting icon on Control Panel
- Blueprint Console
  - Troubleshooting option from the **Open** icon

Troubleshooting tools are the same regardless of which web interface is used



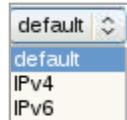
Troubleshooting

© Copyright IBM Corporation 2018

*Figure 8-5. How to get to the Troubleshooting page*

## Troubleshooting: Networking

- Use the **Ping Remote** tool to test connectivity to a remote host
  - Enter IP address or host name and click **Ping Remote**
  - Optionally, enter the IP version to use
  - The default is IPv4
- Use the **TCP Connection Test** to test connectivity to a remote destination
  - Enter IP address or host name
  - Enter the port number
  - Click **TCP Connection Test**



The screenshot shows the IBM DataPower interface under the 'Networking' section. It contains two main sections: 'Ping Remote' and 'TCP Connection Test'. Both sections require a 'Remote Host' input field, which is marked with an asterisk (\*) indicating it is mandatory. In the 'Ping Remote' section, there is also a 'Use IP version' dropdown menu with options: 'default', 'IPv4', and 'IPv6', with 'default' currently selected. A 'Ping Remote' button is located below these fields. In the 'TCP Connection Test' section, there is a 'Remote Port' input field marked with an asterisk (\*), a 'Use IP version' dropdown menu with options: 'default', 'IPv4', and 'IPv6', with 'default' currently selected, and a 'TCP Connection Test' button below it. At the bottom of the interface, there is a navigation bar with the 'Troubleshooting' link and a copyright notice: '© Copyright IBM Corporation 2018'.

Figure 8-6. Troubleshooting: Networking

**Ping Remote** allows DataPower to ping a host system. Use ping to confirm network connectivity to the host IP address that the DataPower gateway is attempting to reach. Intervening servers and firewalls might block ping requests.

The **TCP Connection Test** confirms that DataPower can reach the IP address and the port. This step is useful to confirm whether a service is running remotely or not. For example, you can use TCP Connection Test with the IP address of 0.0.0.0 and port 80 to confirm that the web server is up and running.

## Troubleshooting: Packet capture

- Available in default domain only
- Captures the IP packets sent to and from the gateway
  - Captures full network-level exchange between the gateway and other endpoints
  - Captured in pcap format
  - Tools such as Wireshark can be used to view the traffic in detail
- Useful when troubleshooting network connectivity, TCP sequencing, or other network-level problems
- The packet capture file is available from the **temporary:** directory

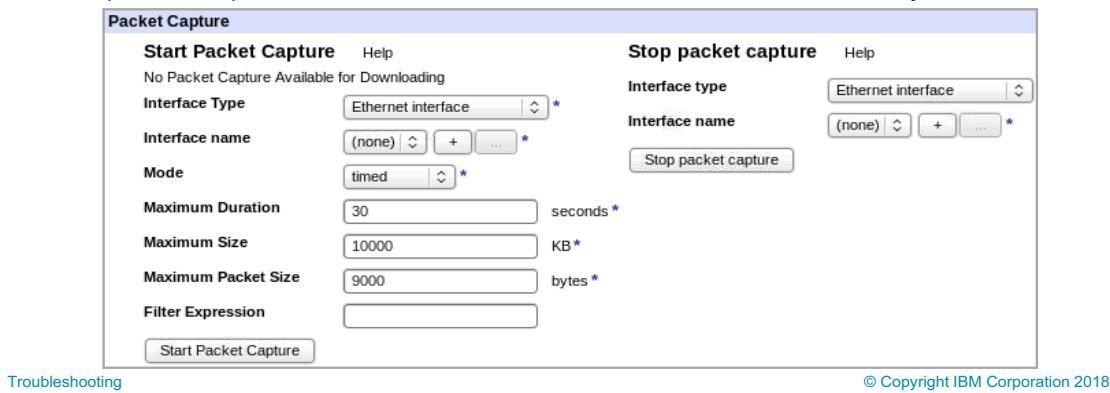


Figure 8-7. Troubleshooting: Packet capture

On the Troubleshooting web page, scroll down to the packet capture section. Click the **Packet Capture** icon to begin the capture. A dialog box confirms the action. When the capture is complete, a **Download Packet Capture** icon appears on the Troubleshooting page.

You can control the network interface to monitor the duration of monitoring and the number of KB that can be captured.

DataPower support expects the pcap format when a PMR is opened.

Before installing a packet capture tool, such as Wireshark (formerly called Ethereal), make sure that you have the necessary permission from your network staff.

Restarting the device automatically turns off packet capture.

## Troubleshooting: Logging

- Use **Set Log Level** to set the log level for the current domain
- Use **Generate Log Event** to verify that log targets are active and able to capture events



[Troubleshooting](#)

© Copyright IBM Corporation 2018

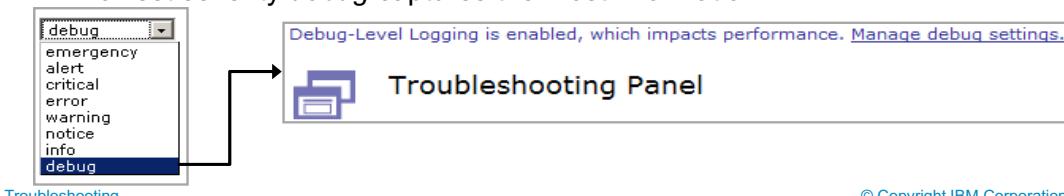
Figure 8-8. Troubleshooting: Logging

Setting the log level to **debug** is helpful during development but it affects processing. Therefore, **debug** mode should not be used in production.

**Generate Log Event** is usually used to test that a log target is configured properly.

## Troubleshooting: System log

- Displays system-wide log messages that the gateway generates
  - Click the **View Logs** icon in the Control Panel
    - In the Troubleshooting pane, scroll down to the Logging section and click **View System Logs**
    - In the Blueprint Console, click **Open > Logs**
- By default, log messages are captured only with severity of *notice* or higher
  - Log levels are hierarchical
  - Highest severity is *emergency*
  - Each level captures messages at or above the current level
  - Lowest severity *debug* captures the most information



© Copyright IBM Corporation 2018

Figure 8-9. Troubleshooting: System log

The highest priority is **emergency** and the lowest priority is **debug**.

The target captures messages only at or above the configured level. For example, the error level captures messages at the error, critical, alert, and emergency levels. To capture all messages, set the log level to **debug**.

Setting the level to either **info** or **debug** causes a blue **Troubleshooting Enabled** notice to appear on all the Web Management pages.

The log levels of the default system log are:

- **emergency**: An emergency-level message. The system is unusable.
- **alert**: An alert-level message. Immediate action must be taken.
- **critical**: A critical message. Immediate action must be taken.
- **error**: An error message. Processing might continue, but action should be taken.
- **warning**: A warning message. Processing should continue, but action should be taken.
- **notice**: A notice message. Processing continues, but action might need to be taken.
- **information**: An information message. No action is required.
- **debug**: A debug message for processing information to help during troubleshooting.

## Filtering system log

- In the default domain, the system log shows all log entries
  - In non-default domains, log entries are shown only for the objects in that domain
- Filter the system log by:
  - Log target
  - Domain (shown only in the default domain)
  - DataPower objects (mpgw, ws-proxy, and more)
  - Log level type (debug, info, and more)

The screenshot shows the 'System Log' interface with the following details:

- Header:** Refresh Log, Target: default-log, Filter: (none), Show last 50 100 all.
- Time:** current time: 13:33:32 on 2012-08-28
- Table Headers:** time, category, level, tid, direction, client, msgid, message.
- Table Rows:**
  - Tue Aug 28 2012
  - 13:32:27 memory-report debug 25568737 171 mpgw response Finished: memory used 616424
  - 13:32:27 mpgw info 25568737 error 172.16.80.11 0x80e000b6 mpgw (EastAddressSearch): No match from processing policy 'EastAddressSearch' for code '0x00230001'
  - 13:32:27 mpgw notice 25568737 172.16.80.11 0x80c0007b stylepolicy (EastAddressSearch): No error rule is matched.
  - 13:32:27 mpgw error 25568737 error 172.16.80.11 0x00230001 mpgw (EastAddressSearch): Dynamic Execution Error
- Buttons:** Category, Log level.
- Bottom:** Troubleshooting, © Copyright IBM Corporation 2018

Figure 8-10. Filtering system log

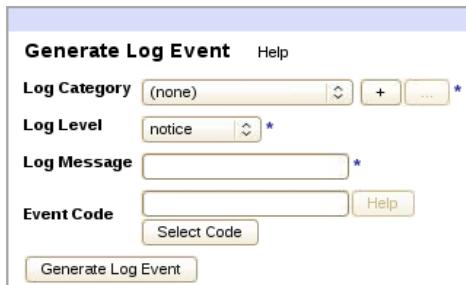
The system log is defined as a log target. A log target receives log entries that DataPower objects generate. Each domain always has a log target that is called **default-log** to represent the default system log. More log targets can be defined and customized with the log entries from objects to post.

The most recent log entries are shown at the top of the system log.

The logs can be sorted by the categories that are listed at the top.

## Troubleshooting: Generate Log Event

- Use the **Generate Log Event** tool to test whether:
  - Log messages are generated in the appropriate log target on the gateway (default system log captures all log messages)
  - Log messages are sent to remote host when off-box logging is used
- Configure log messages with:
  - Log Type: Object class or category
  - Log Level: Debug, info, and other levels
  - Log Message: Text string inside log message
  - Event Code: For generating an event code-based message



Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-11. Troubleshooting: Generate Log Event

The **Generate Log Event** tool is used to test the configuration of a newly created log event and log target.

## Troubleshooting: Reporting

- Generate Error Report
  - Error report is required when engaging with IBM DataPower support
  - Error report file is created in the **temporary:** directory
- Error Report contains:
  - Current configuration
  - Current contents of the system log
  - Contents of CLI log
- Send Error Report:
  - DataPower uses an external mail server (SMTP) to email the error report to a specific email recipient
  - In the Blueprint Console, a **Subject** field replaces the **Location** field

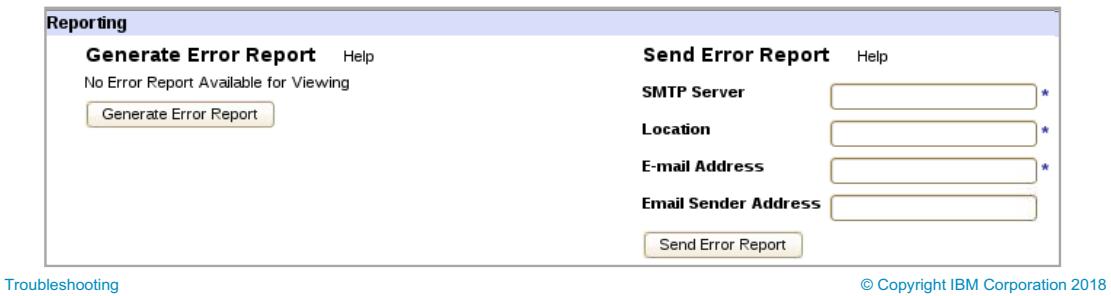


Figure 8-12. Troubleshooting: Reporting

Click **Generate Error Report**. A dialog box prompts for confirmation and indicates the location of the resulting file.

If an error report is available, an icon appears that allows immediate access to the file.

## Troubleshooting: Advanced

- Use XML File Capture to allow the configuration of system-wide file-capture mode
  - The file capture facilitates the visibility of erroneous XML and XSLT content
- Use **View Running Config** to view the configuration of all the objects that are currently in memory



Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-13. Troubleshooting: Advanced

## Troubleshooting: XML File Capture

- Captures XML messages for any service
  - XML messages that services cannot parse can also be captured
- File capture can fill the available storage space
  - Files are cycled FIFO
  - Maximum of 5000 files or 200 MB can be captured
  - Stored in compressed format
  - Supported by using RAM-Disk
- XML File Capture must be enabled only in test environments
  - Significant performance penalties are incurred when mode is set to **always default** domain only



Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-14. Troubleshooting: XML File Capture

XML File Capture sets the configuration of system-wide file-capture mode. The file capture facilitates the visibility of erroneous XML and XSLT content.

## Troubleshooting: Send a test message

The screenshot shows the 'Send a Test Message' tool within the DataPower Gateway. The interface is organized into two main sections: 'Request' and 'Response'. The 'Request' section contains fields for 'URL', 'Request Headers' (a table with columns 'Header Name' and 'Value'), and 'Request Body'. The 'Response' section displays 'Response Code', 'Response Headers', and 'Response Body'. Four yellow circles with numbers 1 through 4 are overlaid on the interface to point out specific features: 1 points to the URL input field, 2 points to the Request Headers table, 3 points to the Request Body input field, and 4 points to the Response area.

- WebGUI and Blueprint Console: **Administration > Debug > Send a Test Message**
- Builds a request with a customized header, content, and body that is used for testing
  1. A URL can be generated by using the different helpers
  2. Request headers can be added
  3. A request body can be typed or pasted here
  4. The response is displayed here

© Copyright IBM Corporation 2018

Figure 8-15. Troubleshooting: Send a test message



### Note

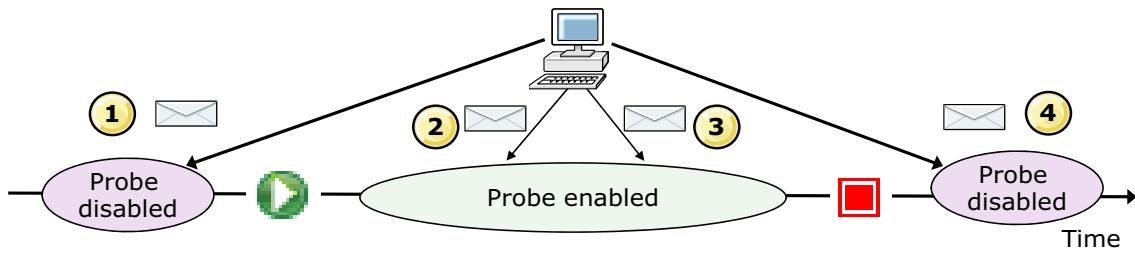
You might need to allow pop-ups in the browser before the test message dialog is displayed.

#### Using the **Send a test message** tool versus **cURL**:

The test message tool is a quick and useful tool for sending requests, and it can be used in place of open source tools like cURL. However, when using the test message tool, you cannot upload a file to the DataPower box to send; you need to copy and paste text. You also cannot persist the test message after it is created. The advantage of using tools like cURL is that it can send files directly from the file system.

## Troubleshooting: Multi-step probe

- Displays the lifecycle of the message as it runs in a processing rule
  - Information is captured after processing rule runs
- Aids in debugging processing rules
  - Step-by-step debugging to view message content after execution of each action in the processing rule
  - Enable only in test environment because it impacts gateway performance



Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-16. Troubleshooting: Multi-step probe

In the diagram on the slide, four messages are sent to the probe. Only message 2 and message 3 are captured. The probe functions like a recorder. When the probe is enabled, it starts recording messages that enter the gateway. When the probe is disabled, recording is stopped and the probe stops capturing messages.

The multi-step probe can be used to view:

- Action execution trace
- Message content
- Header values
- Attachments
- Variable values (local, context, global, service)



## Troubleshooting: Enabling the multi-step probe

Two ways to enable a probe for a service:

- Click the **Debug Probe** tab on the Troubleshooting page
- Click **Add Probe** to add a probe for that service
- On the service configuration page, click the **Show Probe** button (WebGUI) or **Actions > Show Probe** (Blueprint Console) to open the probe transaction list window

The screenshot shows the 'Actions' dropdown menu for a service named 'MyBasicMPG'. The 'Show Probe' option is highlighted with a red box.

Troubleshooting © Copyright IBM Corporation 2018

Figure 8-17. Troubleshooting: Enabling the multi-step probe

Enable the probe in either of two ways from the Blueprint Console:

1. From the Troubleshooting, click the Debug Probe link. Then, click Add Probe to add the probe for the service.
2. From the Services icon, select All Services. Then, click to open the service. When the service is displayed, select Show probe from the Actions menu.

IBM Training IBM

## Multi-step probe transaction list

- Enable the probe in the transaction list window
  - Send messages to the service
  - Click **Refresh** in the transaction list window
  - Examine the captured request and response rule processing results

**View probe data**

view	trans#	type	inbound-url	outbound-url	rule
	92114	request	http://192.168.100.201:10016/	http://192.168.100.201:10016/	MyBasicMPG_rule_2

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-18. Multi-step probe transaction list

The transaction list window opens with the probe disabled when you show the probe from the service configuration page.

Rules that generate an error while executing are displayed in red text.

Clicking **Flush** clears the requests inside the transaction list.

Restarting the gateway disables all probes.

By clicking **Export Capture** in the transaction list window, you can download the service configuration and files that are used in execution of the rule. Download the .zip file and send it to support when you have problems with a service policy.

Step 1: Transform with XSLT style sheet Action:Input=INPUT, Transform=store:///identity.xsl, ParseSettingsReference= , Pai TransformLanguage=none, ActionDebug=off, Output=dpvvar\_10, NamedInOutLocationType=default, SSLClientConfigType= Transactional=off, SOAPValidation=body, SQLSourceType=static, JWSServerSignature=on, Asynchronous=off, Res RetryCount=0, RetryInterval=1000, MultipleOutputs=off, IteratorType=XPATH, Timeout=0, MethodRewriteType=GET, MethodType2=POST

**Content** **Headers** **Attachments** **Local Variables** **Context Variables** **Global Variables**

**Content of context 'INPUT':**

```
<address:getAddressInfo
 xmlns:address="http://dpedu.ibm.com"
>
<address:name>
 <address:title>Mr.</address:title>
 <address:firstName>John</address:firstName>
 <address:lastName>Doe</address:lastName>
</address:name>
</address:getAddressInfo>
```

- View the message content as it traverses each action
- Each action has an input and output message that can be viewed by clicking the magnifying glass
  - Message content
  - Protocol headers and message attachments
  - Local, context, global, and service variables
  - Actions that the processing rule runs

Troubleshooting © Copyright IBM Corporation 2018

Figure 8-19. Multi-step probe content

- The row of actions across the top show what executed in the rule. The magnifying glass to the left of the action represents the input message. The magnifying glass to the right of the action is the result of executing that action. When you click a particular magnifying glass, the contents of the rest of the page changes to the state at that point in the processing. The square brackets around the magnifying glass indicate which one is selected. You can also click **Next** and **Previous** to view the message step-by-step as it is executed from the processing rule.
- The default tab that is displayed is the **Content** tab. The tab renders the message contents if it can.
- Other tabs are available to show more state that is associated with the message processing at the selected point in the rule.

The local, context, global, and service variables are DataPower variables that are generated from the gateway.

## Debugging GatewayScript (1 of 4)

- To activate the GatewayScript debugging, two conditions must be met:
  - Debugging must be enabled in the GatewayScript action
  - The script that is in the GatewayScript Action must contain a “debugger;” statement

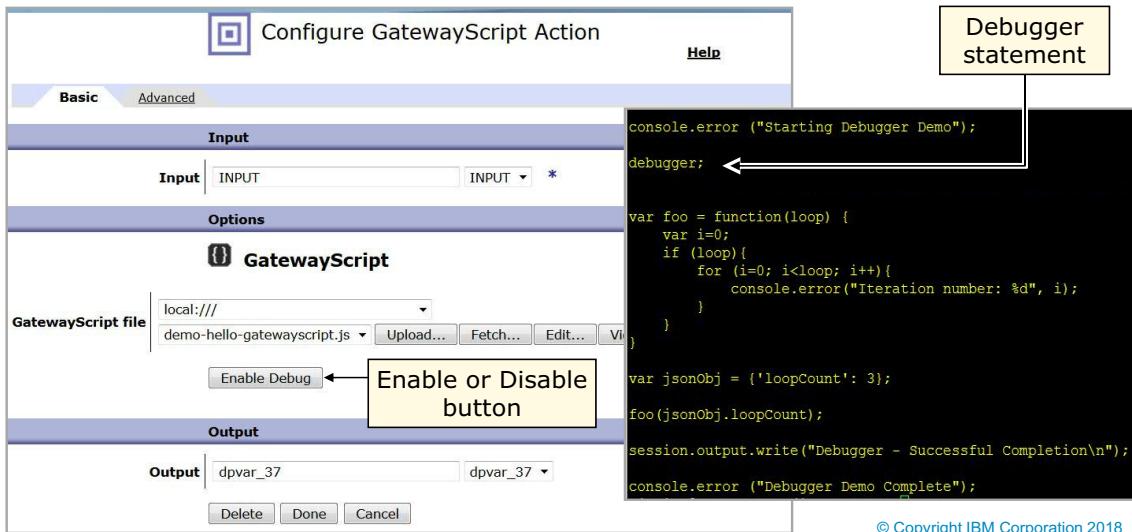


Figure 8-20. Debugging GatewayScript (1 of 4)

To activate the GatewayScript debugger, two conditions must be met. The first condition requires the GatewayScript debugging to be enabled. GatewayScript debugging is enabled by clicking **Enable Debug** in the configuration screen of the GatewayScript action. The enable or disable button is highlighted in the image on the left side of this slide.

The **Debug** button does not persist during a domain or gateway reboot. Therefore, if the button was enabled, and the gateway is rebooted, the button is in a disabled state after the reboot.

The second condition that must be met requires the syntax of the GatewayScript code to contain the debugger statement. An example is represented in the image that is on the right side of the screen.

## Debugging GatewayScript (2 of 4)

- The flow of a transaction is paused indefinitely
  - The GatewayScript processing breaks at the “debugger ;” line
  - A maximum of 10 debug sessions are in progress at any time
  - Use “show debug-actions” (in config mode) to find available sessions to debug

```
xi50[2459-GatewayScript](config)# show debug-actions

Session ID Transaction ID Service Name File Location
Remote Address In Use Remote User User Location Elapsed Time
----- ----- -----
85 63553 GatewayScript-Loopback local:///demo-debugger.js
127.0.0.1 No 00:06:43

xi50[2459-GatewayScript](config)#

```

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-21. Debugging GatewayScript (2 of 4)

This screen capture image is an example of what you would see and how you would figure out how to begin the debugger. When debugging is enabled, and a debugger statement exists in the GatewayScript script, a “*show debug-actions*” message shows the debug requests.

The GatewayScript execution pauses at the debugger statement. You might have up to 10 debug sessions in progress at one time. The scope of the maximum debug sessions is per gateway (not per domain).

- The session ID is used to identify which debug session you want to work with.
- The transaction ID is the ID of the transaction.
- The service name is the name of the service.
- The file location is the actual location of the script file that is being paused.
- The remote address is the address of the client.

**In Use** represents whether someone else is debugging the session. Currently, joint debugging is not allowed, so if **In Use** is set to Yes, you cannot debug this session.

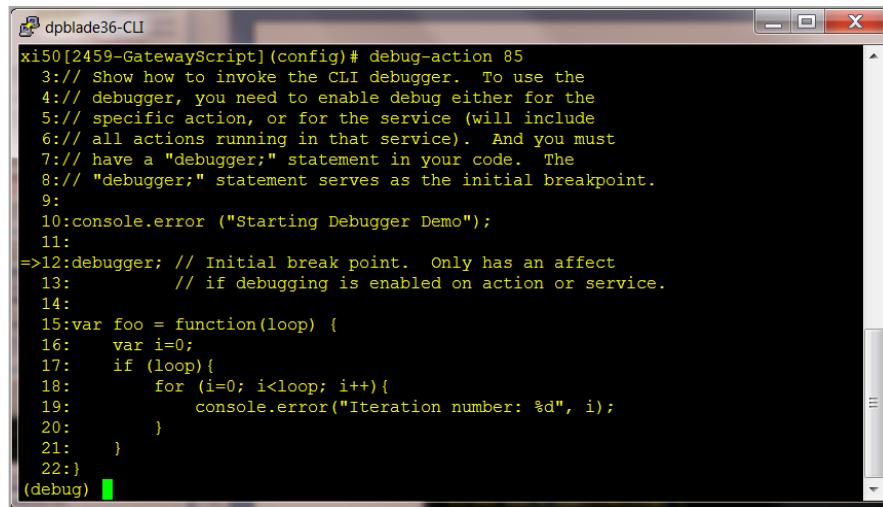
If **In Use** is Yes, then the following fields contain data that represents the user currently debugging the session:

- User: The user currently debugging the session

- User location: IP address of the user
- Elapsed time: The amount of time that the transaction remains in the debugger

## Debugging GatewayScript (3 of 4)

- Enter the CLI debugger: GDB-like interface
  - Must be in config mode in the domain where the action executed
  - debug-action <session ID>: Enter the CLI debugger until the script completes



```

xi50[2459-GatewayScript] (config)#
 3:// Show how to invoke the CLI debugger. To use the
 4:// debugger, you need to enable debug either for the
 5:// specific action, or for the service (will include
 6:// all actions running in that service). And you must
 7:// have a "debugger;" statement in your code. The
 8:// "debugger;" statement serves as the initial breakpoint.
 9:
 10:console.error ("Starting Debugger Demo");
 11:
=>12:debugger; // Initial break point. Only has an affect
 13: // if debugging is enabled on action or service.
 14:
 15:var foo = function(loop) {
 16: var i=0;
 17: if (loop){
 18: for (i=0; i<loop; i++){
 19: console.error("Iteration number: %d", i);
 20: }
 21: }
 22:}
(debug)

```

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-22. Debugging GatewayScript (3 of 4)

The GatewayScript debugger is similar to the GNU Project debugger (GDB), which shows what is going on inside another program while it is running.

The **debug-action** must be executed from within the domain that is being debugged, and from within configuration mode (use the CLI `co` command).

The previous slide showed a debug session ID of 85. This image shows how you enter a debugging session, by executing a debug-action and the session ID: `debug-action 85`

What you are going to see, as represented on the image, is that the debugger shows a listing of the code around the debug statement. The debug listing includes line numbers and an arrow `=>` pointing to the debug statement.

In the debugger, many commands can be executed, such as step-into, step-over, and other commands. The debugger commands are listed on the next slide.

## Debugging GatewayScript (4 of 4)

### Debugging commands:

- List source code
  - `list(l) [number of lines]`
- Breakpoints
  - `break (b) <line | script.js:line | function()>`
  - `delete (d) <identifier | all>`
  - `info break (ib)`
- Print variable values
  - `print (p) <variable>`
- Explore stack trace
  - `backtrace (bt)`
- Program execution control
  - `continue (c)`
  - `next (n) [count]`
  - `step (n) [count]`
  - `out (o) [count]`
  - `quit (q)`

[Troubleshooting](#)

© Copyright IBM Corporation 2018

Figure 8-23. Debugging GatewayScript (4 of 4)

This slide includes a list of some of the GatewayScript debugging commands that the debugger supports.

For more information, see the “GatewayScript debugger commands” section in the DataPower Gateways Knowledge Center.

## Problem determination with cURL

- Use cURL with **-v** option to output more information to trace client-side errors
  - This option is independent of the DataPower gateway troubleshooting tool
- Use the **--trace** or **--trace-ascii** option with a file name to write the logging data
  - Provides more details on the client/server interaction
- Sample tracing with cURL:

```
curl --trace-ascii trace1.txt
 -D headers1.txt
 -H "Content-Type:text/xml"
 -d @AddressReq.xml
 http://dpedu1:2064
```

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-24. Problem determination with cURL

The **-v** verbose flag produces much information in the output. It allows the user to see all of the client and server interaction.

## Communicating with DataPower support

- DataPower support information links are at the bottom of the Control Panel page
- “Contacting IBM WebSphere Appliance Support” technical note:
  - <http://www.ibm.com/support/docview.wss?uid=swg21236322>
- Generally, use the Troubleshooting page to supply DataPower support with the following files:
  - The DataPower error report
  - The running configuration

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-25. Communicating with DataPower support

## Unit summary

- Identify the troubleshooting tools that are available on the DataPower appliance
- Capture information by using system logs for messages that pass through the DataPower gateway
- Configure the default system log for debugging
- Configure a multi-step probe to examine detailed information about actions within rules

Troubleshooting

© Copyright IBM Corporation 2018

*Figure 8-26. Unit summary*

## Review questions

1. You want to find out whether you can reach a particular host name. What DataPower facility can you use?
  - A. Troubleshooting > Ping Remote
  - B. Troubleshooting > XML File Capture
  - C. Troubleshooting > Generate Log Event
  - D. Use cURL with **-v** option
2. **True or False.** System administrator authority is required to enable Packet Capture.
3. A message is getting an XML parsing error. Which DataPower tool can you use to see the XML content as received?
  - A. Troubleshooting > Ping Remote
  - B. Troubleshooting > XML File Capture
  - C. Troubleshooting > Generate Log Event
  - D. Use cURL with **-v** option
4. **True or False.** The multistep probe captures information after a processing rule runs.

Troubleshooting

© Copyright IBM Corporation 2018

Figure 8-27. Review questions

Write your answers here:

- 1.
- 2.
- 3.
- 4.

## Review answers

1. **A.** You want to find out whether you can reach a particular host name. What DataPower facility can you use?

- A.Troubleshooting > Ping Remote**  
B. Troubleshooting > XML File Capture  
C. Troubleshooting > Generate Log Event  
D. Use cURL with **-v** option

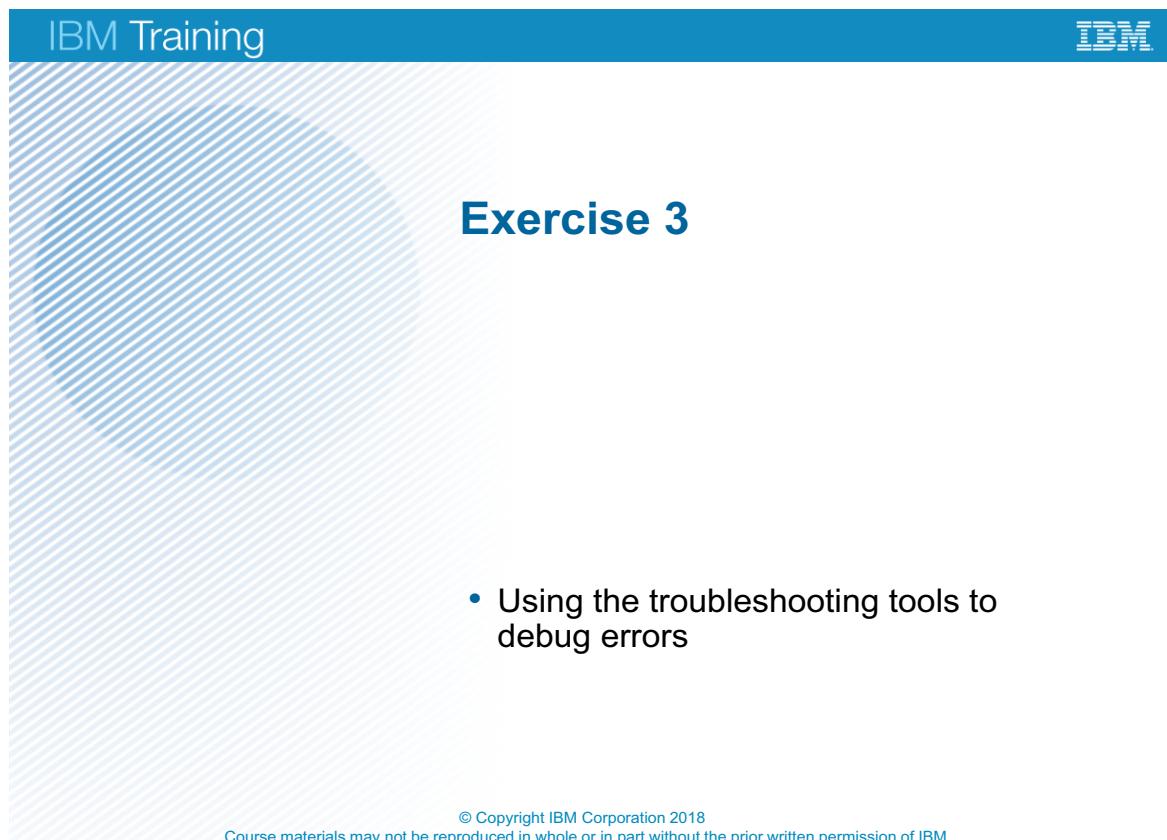
2. **True.** System administrator authority is required to enable Packet Capture.

3. **B.** A message is getting an XML parsing error. Which DataPower tool can you use to see the XML content as received?  
**B.Troubleshooting > XML File Capture**  
A. Troubleshooting > Ping Remote  
C. Troubleshooting > Generate Log Event  
D. Use cURL with **-v** option

4. **True.** The multistep probe captures information after a processing rule runs.

Troubleshooting © Copyright IBM Corporation 2018

Figure 8-28. Review answers



The slide features a blue header bar with 'IBM Training' on the left and the IBM logo on the right. Below the header is a large, light blue diagonal striped area. In the center of the slide, the text 'Exercise 3' is displayed in a bold, dark blue font. To the right of the striped area, there is a bulleted list: '• Using the troubleshooting tools to debug errors'. At the bottom right of the slide, there is a copyright notice: '© Copyright IBM Corporation 2018' and 'Course materials may not be reproduced in whole or in part without the prior written permission of IBM.'

- Using the troubleshooting tools to debug errors

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Figure 8-29. Exercise 3

## Exercise objectives

After completing this exercise, you should be able to:

- Set up and analyze the default system logs
- Configure a multi-step probe to conduct message-level process debugging

*Figure 8-30. Exercise objectives*

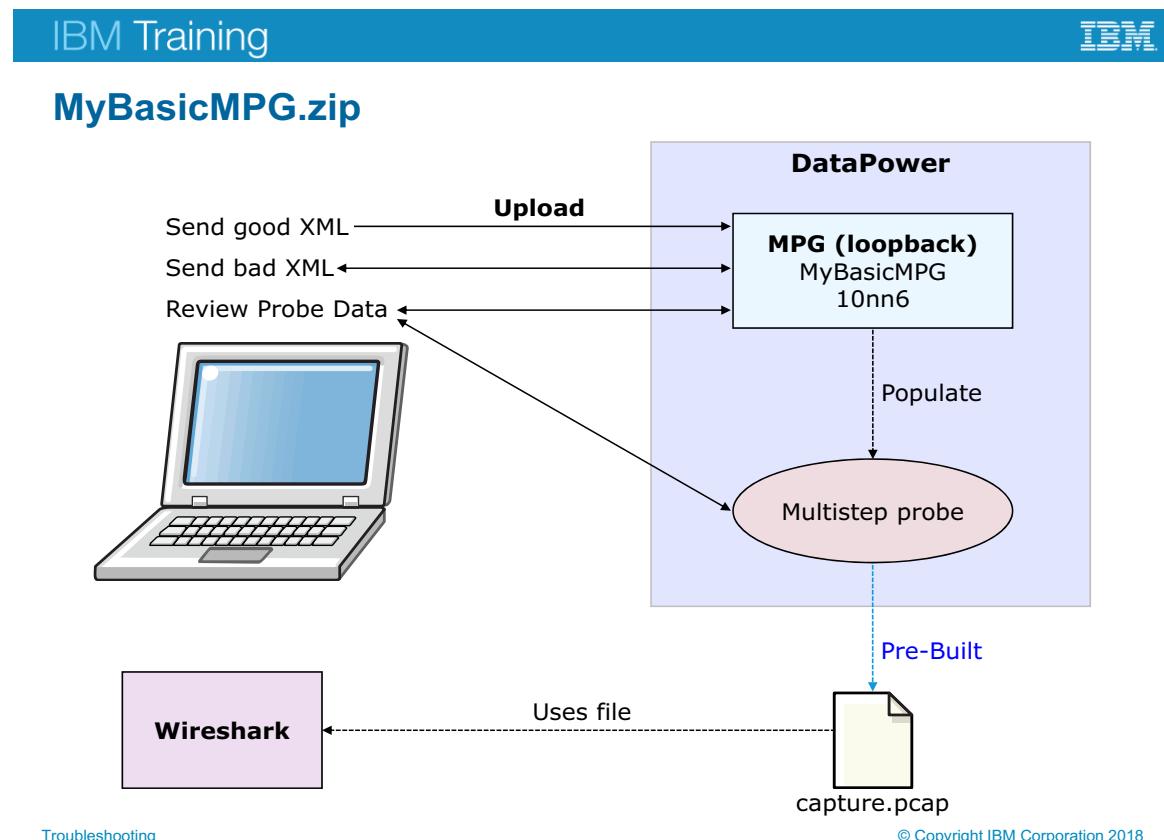


Figure 8-31. *MyBasicMPG.zip*

First, the MyBasicMPG multi-protocol gateway service is uploaded to the students domain. Next, the MPG is configured with the correct port number.

The MPG is then used to receive a valid XML message and a non-valid XML message. The system logs and multistep probe are used as debugging tools.

Finally, a precapture pcap file is analyzed by using the Ethereal tool.

---

# Unit 9. DataPower cryptographic tools and SSL setup

## Estimated time

01:00

## Overview

This unit describes how to use the cryptographic tools to create keys and certificates. You learn how to set up the DataPower objects that are used to validate certificates and configure certificate monitoring to ensure that only valid certificates exist on the appliance. Finally, you learn how to secure connections by using SSL to and from the DataPower appliance.

## How you will check your progress

- Review questions
- Lab exercise

## References

IBM DataPower Gateways 7.6.0 product documentation:

[https://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0/com.ibm.dp.doc/welcome.html](https://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0/com.ibm.dp.doc/welcome.html)

## Unit objectives

- Explain how to use the DataPower tools to generate cryptographic keys
- Create a cryptographic identification credential object that contains a matching public and private key
- Create a cryptographic validation credential to validate certificates
- Set up certificate monitoring to ensure that certificates are up-to-date
- Configure an SSL server profile that accepts an SSL connection request from a client
- Configure an SSL client profile that initiates an SSL connection from a DataPower service
- Configure an SSL SNI server profile that supports SNI requests

Figure 9-1. Unit objectives

## DataPower use of keys and certificates

- DataPower supports asymmetric keys (private key – public key/certificate) and symmetric keys
- Keys are used for:
  - SSL/TLS communications
  - Digital signatures
  - Encryption
- Numerous DataPower objects to support the keys and relationships
- Several functions in Blueprint Console or WebGUI **Crypto Tools** to help with working with keys

Figure 9-2. DataPower use of keys and certificates

Secure Socket Layer (SSL) is a cryptographic protocol to secure communications over the network. Transport Layer Security (TLS) is its successor. The term “SSL” typically refers to both protocols.

## Creating a private key and certificate

- Methods for creating a private cryptographic key and a self-signed digital certificate:
  - Generated onboard using the DataPower Crypto Tools
    - Administration > Miscellaneous > Crypto Tools
  - Uploading key files that are generated on a workstation to the DataPower gateway
    - Example: openSSL

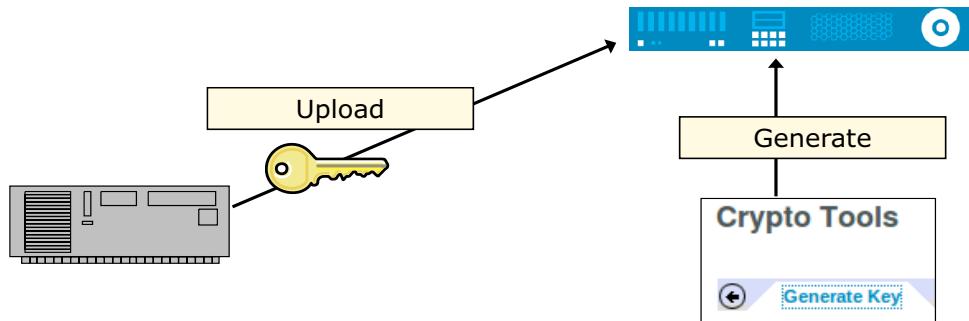


Figure 9-3. Creating a private key and certificate

Crypto Tools do not generate symmetric keys. Symmetric algorithms use the same key for both encryption and decryption.

Asymmetric algorithms, also called public keys, use different keys for encryption and decryption.

Recall that the digital certificate contains the public key.

## Generating crypto (asymmetric) keys onboard (1 of 2)

In the Blueprint Console, expand **Administration** and click **Miscellaneous > Crypto Tools**

- Enter key information, only **Common Name (CN)** is required
- Both RSA and ECDSA keys are supported
  - RSA prompts for **key length** (1024 – 4096 bits) and **hash algorithm**
  - ECDSA prompts for **elliptic curve**

Generate Key	
LDAP (reverse) Order of RDNs	<input type="radio"/> on <input checked="" type="radio"/> off
Country Name (C)	<input type="text"/>
State or Province (ST)	<input type="text"/>
Locality (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organizational Unit (OU)	<input type="text"/>
Organizational Unit 2 (OU)	<input type="text"/>
Organizational Unit 3 (OU)	<input type="text"/>
Organizational Unit 4 (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Key type	RSA
RSA key length	1024 bits *
Hash Algorithm	sha256
File Name	<input type="text"/>

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-4. Generating crypto (asymmetric) keys onboard (1 of 2)

The files that are submitted to a certificate authority, including the certificate signing request (CSR) file, are created by default.

The fields from **Country Name (C)** down to **Common Name (CN)** are part of the distinguished name.

The file name for the private key, CSR, and self-signed certificate that is generated uses the **File Name** field for its prefix. If the **File Name** field is left blank, the system uses the value from the **Object Name** field.

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.

The ECDSA (Elliptic Curve Digital Signature Algorithm), relies on a private key in the authenticator and a public key that the host uses to verify the authenticator.

If you generate an RSA key, you must define the key length and the hash algorithm of the generated RSA keys. If you generate an **ECDSA** key, you must define the elliptic curve to use to generate the **ECDSA** keys.

## Generating crypto (asymmetric) keys onboard (2 of 2)

- Keys cannot be exported from the DataPower gateway to the workstation
  - Except, when **Export Private Key** is selected
  - Exported to `temporary:` directory
- Generated key and certificate objects use the name that is entered in the optional **Object Name** field, otherwise the name in the CN field
- Click **Generate Key** to generate the key and certificate files and objects

The screenshot shows a configuration dialog for generating keys. It includes fields for 'Validity Period' (set to 365), 'Password Alias' (set to '(none)'), and 'Object Name'. There are three radio buttons for generating certificates: 'Generate Self-Signed Certificate', 'Export Self-Signed Certificate', and 'Generate Key and Certificate Objects'. The 'Generate Key and Certificate Objects' option is selected. At the bottom is a 'Generate Key' button.

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-5. Generating crypto (asymmetric) keys onboard (2 of 2)

Password Alias specifies the existing password alias map that defines the alias that maps to the clear text password. The password in the map encrypts the files, and the alias in the map decrypts the password to access the file.

Select **on** for **Generate Self-Signed Certificate** to generate a self-signed certificate into the `temporary:` directory and the `store:` directory.

If **Export Self-Signed Certificate** or **Export Private Key** is **off**, then the generated key or certificate is placed in the `cert:` directory only, where it cannot be edited.

When you click **Generate Key**, you generate a private key file and object, and a certificate file and object.

## Download keys from temporary storage

- Keys can be downloaded from temporary storage when **Export Private Key** or **Export Self-Signed Certificate** is on
- Expand the **temporary:** folder in **File Management**
- Right-click the file and click **Save Target As**

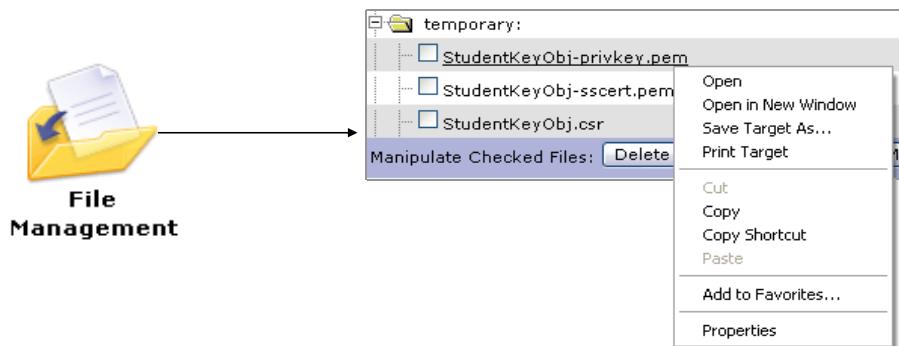
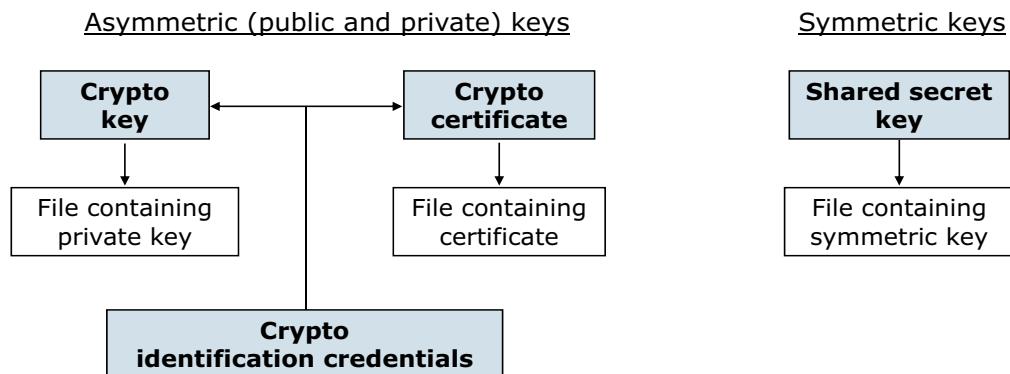


Figure 9-6. Download keys from temporary storage

The `temporary:` directory is cleared when the gateway shuts down or restarts.

## Key and certificate objects point to files

- The key and certificate objects point to the files on the gateway that are the actual key or certificate
  - Certificate contains the public key



- The **crypto identification credentials** object maintains the relationship between the private key object and its related certificate (public key) object

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-7. Key and certificate objects point to files

Although the shared secret key is not used in SSL, it is used in OAuth and OpenID Connect, and infrequently in encryption and signatures.

## Crypto shared secret (symmetric) key

Define a shared secret key object that points to the symmetric key file

- **Objects > Crypto Configuration > Crypto Shared Secret Key**



Figure 9-8. Crypto shared secret (symmetric) key

A shared secret key is used for symmetric key encryption.

Symmetric keys are used in OAuth and OpenID Connect.

DataPower does not have a utility that can generate a symmetric key. Use a tool, such as the Java “keytool” or OpenSSL, to generate a key.

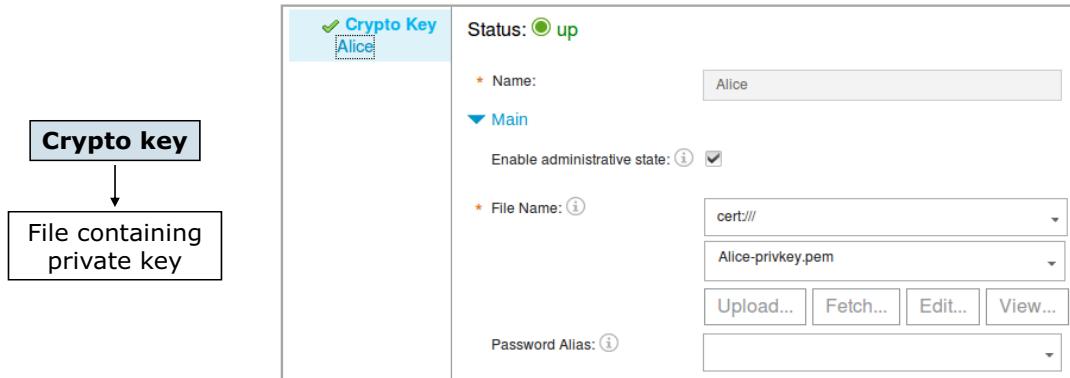
The key file can be uploaded from this page.



## Crypto (asymmetric) key

Define a crypto key object that points to the private key file

- **Objects > Crypto Configuration > Crypto Key**
- Can specify password alias
  - Forces users of key file to supply a password



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-9. Crypto (asymmetric) key

A crypto key represents the private key that is used for asymmetric key encryption.

The key file can be uploaded from this page.

The password alias points to an encrypted clear text password that is required to access the file that contains the private key.



## Crypto certificate

Define a certificate object that points to the certificate file

- **Objects > Crypto Configuration > Crypto Certificate**
- Can specify password alias
  - Forces users of certificate file to supply a password

<b>Crypto certificate</b>  <b>File containing certificate</b>	<div style="border: 1px solid #ccc; padding: 10px;"> <p><b>Crypto Certificate</b> Alice</p> <p>✓ Password Map Alias password</p> <p>Status: <b>up</b></p> <p>* Name: Alice</p> <p>▼ Main</p> <p>Enable administrative state: <input checked="" type="checkbox"/></p> <p>* File Name: cert:/// Alice-sscert.pem</p> <p>Details... Upload... Fetch...</p> <p>Password Alias: password</p> <p>Ignore Expiration Dates: <input type="checkbox"/></p> </div>
---------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-10. Crypto certificate

Setting a **Password Alias** option means that the password that is needed to access the key is stored in a secure password map.

If **Ignore Expiration Dates** is off, the certificate object is placed in a “down” state if it is out of its validity date range. If it is on, the certificate object is in an “up” state, but it might be rejected during processing because of an invalid date.

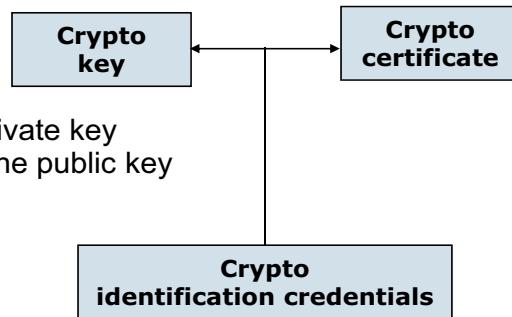


## Crypto identification credential

Create a crypto identification credential

- Maintains the relationship between a private key and its related certificate that contains the public key
- Commonly used for SSL authentication

**Objects > Crypto Configuration > Crypto Identification Credentials**



<b>Crypto Identification Cred</b> AliceIdCred *	* Name: <input type="text" value="AliceIdCred"/> <b>Main</b> Enable administrative state: <input checked="" type="checkbox"/> * Crypto Key: <input type="text" value="Alice"/> * Certificate: <input type="text" value="Alice"/> Intermediate CA Certificate: No items. <input type="button" value="Add"/>
----------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-11. *Crypto identification credential*

In the **Crypto Key** field, select the crypto key object from the list. You can use the **New** or **Edit** icons to create or edit a crypto key object.

In the **Certificate** field, select a certificate object from the list. You can use the **New** or **Edit** icons to create or edit a certificate object.

Specify the intermediate certificate authority (CA) certificates, if available, by clicking **Add**. The process establishes a trust chain that consists of one or more CA certificates.

You can also create a crypto identification credential by clicking **Keys and Certs Management > Identification Credentials** from the Control Panel.

## Example: Display details of a crypto file

- Select **Objects > Crypto Configuration > Crypto Identification Credentials**
- Select the certificate. Then, click **Details** to display the certificate fields

**Details of Crypto File cert:///Alice-sscert.pem**

Basic Fields	
Fingerprint(SHA1)	96:AF:AF:20:1C:21:A3:30:13:89:B5:08:ED:69:2B:13:6E:C9:21:17
Version	3
SerialNumber	7052125777297581617
SignatureAlgorithm	sha256WithRSAEncryption
Issuer	C=US, ST=CA, L=Los Angeles, O=IBM, OU=Software Group, CN=Alice
NotBefore	2018-01-15T23:41:05Z
NotAfter	2028-01-13T23:41:05Z
Subject	C=US, ST=CA, L=Los Angeles, O=IBM, OU=Software Group, CN=Alice
SubjectPublicKeyAlgorithm	rsaEncryption
SubjectPublicKeyBitLength	2048

*Figure 9-12. Example: Display details of a crypto file*

Although you can use a certificate monitor that checks the expiration date of all certificates, you can view certificate details to evaluate other issues that you can encounter during processing that uses certificates.

Viewing certificate details:

In the search field, enter Certificate.

From the search results, click Crypto Certificate.

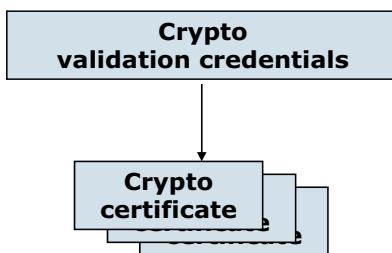
From the table, select a certificate alias to view its configuration.

Click Details beside the file name.



## Crypto validation credential

- Specifies one or more certificates that a presented certificate or digital signature can be verified against
  - Is the certificate valid?
- The validation mode indicates how to validate against the list:
  - Exact certificate or immediate issuer
  - Full certificate chain checking (PKIX)
  - Match exact certificate
- Commonly used for SSL
- Can use certificate revocation lists (CRLs)



DataPower cryptographic tools and SSL setup

✓ Crypto Validation Credential BookingValCred *	* Name: <input type="text" value="BookingValCred"/>
<b>Main</b>	
Enable administrative state: <input checked="" type="checkbox"/>	
Certificates: <input type="button" value="Alice"/> New <input type="button" value="Add"/>	
Certificate Validation Mode: <input type="radio"/> Match exact certificate or immediate issuer	
Use CRL: <input checked="" type="checkbox"/>	
Require CRL: <input type="checkbox"/>	
CRL Distribution Points Handling: <input type="radio"/> Ignore	
Check Dates: <input checked="" type="checkbox"/>	

© Copyright IBM Corporation 2018

Figure 9-13. Crypto validation credential

The certificate validation mode specifies how to validate the presented certificate.

Two options are available:

- Match exact certificates or immediate issuer:** The certificate that is presented or the immediate issuer of the certificate must be available on the gateway.
- Full certificate chain checking (PKIX):** The certificate that is presented and any intermediate certificates that are chained back to the root certificate must be trusted.
- Match exact certificate:** The validation credentials contain the exact peer certificate to match.

The **Use CRLs** field is used to check whether certificates in the trust chain should be monitored for revocation.

## Import and export crypto objects

### In Crypto Tools

- Export a **certificate** object to a file
  - The XML file is exported to `temporary:` directory on the gateway
- Import Crypto Object brings in the exported **certificate** object
  - The XML file can be in another directory or uploaded
- Private keys can be exported or imported for HSM-equipped gateways only
- The raw key files cannot be exported from the `cert:` directory
- Key files can be uploaded to the gateway either in File Management or by using the **Upload** button

Figure 9-14. Import and export crypto objects

This page is accessed **Administration > Miscellaneous > Crypto Tools**.

Certificates are exported to the `temporary:` directory. They can be downloaded by using file management.

Only certificates can be exported and imported.

The object name that is typed must match the name of the exported crypto object exactly.

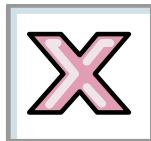
For an imported crypto object, a password alias can be supplied if the password is not entered.

If the gateway has the Hardware Security Module (HSM) feature installed, private keys can be exported and imported.

## Certificates can expire or get revoked



- Certificates are valid only for a certain length of time *and can expire*
- A **certificate monitor** can constantly check certificates that are stored on the gateway and warn before expiration invalidates the certificate
  - This object is *up* by default



- The issuing authority can also revoke certificates
- The gateway can check **certificate revocation lists** (CRL) for revoked certificates

Figure 9-15. Certificates can expire or get revoked

## Certificate revocation list (CRL) retrieval

- A certificate revocation list (CRL) is a list of certificates from a specific certificate authority (CA) that are revoked and are no longer valid
  - You need to periodically check the validity of certificates
  - Supports CRLs that are in the DER format only
- To set up a CRL list from the vertical navigation bar, click **Objects > Crypto Configuration > CRL Retrieval**
- In the CRL Retrieval object, create a **CRL update policy** for each CRL to be monitored
  - Can use HTTP or LDAP to retrieve the list
  - Specify refresh interval
- Is visible and configurable in the **default** domain only

* Policy Name: <input type="text"/>	<input type="button" value="..."/>
* Protocol: <input type="text"/>	HTTP <input type="button" value="..."/>
* CRL Issuer Validation Credentials: <input type="text"/>	<input type="button" value="..."/> <input type="button" value="+"/>
* Refresh Interval: <input type="text"/>	240 minutes
SSL client type: <input type="text"/>	Proxy Profile <input type="button" value="..."/>
Cryptographic Profile (deprecated): <input type="text"/>	
* Fetch URL: <input type="text"/>	<input type="button" value="..."/>

Figure 9-16. Certificate revocation list (CRL) retrieval

Any trust chain that uses a revoked certificate is broken.

A CRL policy can be configured to fetch CRL lists from a CRL server. The CRL server is checked for validity by using the **CRL Issuer Validation Credential** object that is selected.

The protocol is either **HTTP** or **LDAP**. Appropriate fields must be completed to support the protocol.

SSL fields are available to create an SSL session for the HTTP or LDAP connection to the CRL server.

## Crypto certificate monitor

- Periodic task that runs on the gateway that checks the expiration date of certificates
- **Objects > Crypto Configuration > Crypto Certificate Monitor**
- Expiring certificates are identified in a log file with a specified warning
- Is visible and configurable in the **default** domain only

**Crypto Certificate Monitor**

Status:  up

▼ Main

Enable administrative state:	<input checked="" type="checkbox"/>
Comments:	<input type="text"/>
* Polling Interval:	<input type="text"/> 1 day
* Reminder Time:	<input type="text"/> 30 day
* Log Level:	<input type="button"/> warning
* Disable Expired Certificates:	<input type="checkbox"/>

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

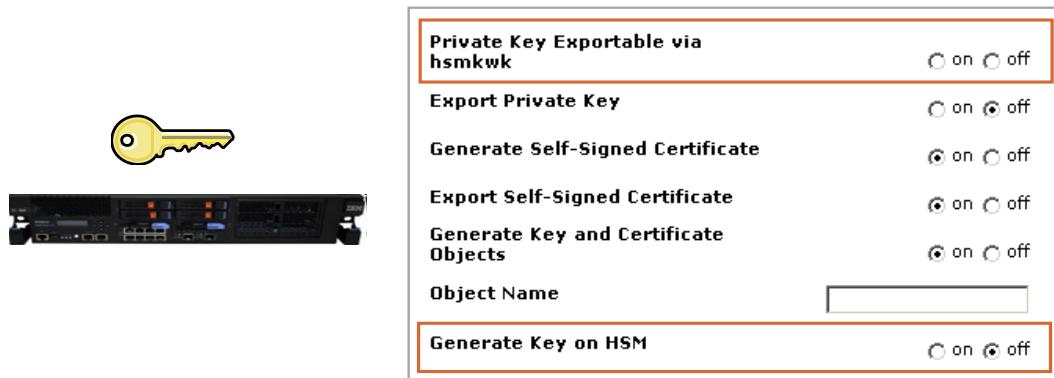
Figure 9-17. *Crypto certificate monitor*

Polling interval specifies the frequency at which certificate expiration dates are checked.

Reminder time is the number of days before the certificate expiration that event is written to the log file.

## Hardware Security Module (HSM)

- Physical gateways with a hardware security module (HSM) installed can export and import private keys
  - The gateway where the key is exported or imported must also have HSM hardware that is installed
- The HSM accelerates RSA operations
- DataPower supports FIPS 140-2 level 3 security



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-18. Hardware Security Module (HSM)

An HSM-equipped appliance supports the following operations:

- Accelerate synchronous and asynchronous RSA operations: Sign, verify, encrypt, and decrypt.
- Encrypted password-based login.
- Generate and store RSA private keys on the HSM.
- Export and import key material among HSM-equipped appliances. Appliances must share a key-wrapping key and belong to the same key-sharing domain.
- Delete RSA private keys from the HSM.

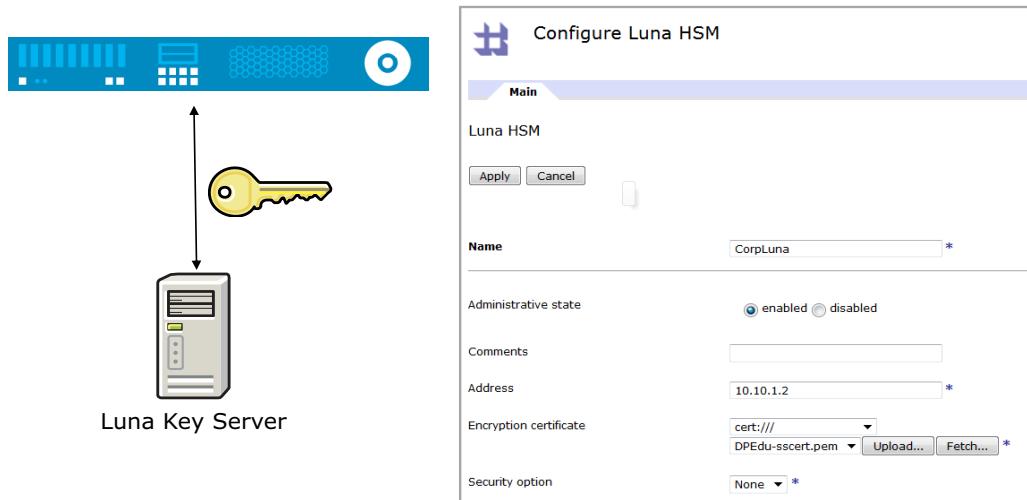
The HSM option is shown only if a physical HSM is installed.

Generating keys on HSM is not available on a virtual gateway.



## Remote Hardware Security Module (HSM)

- The SafeNet Luna Network HSM provides HSM capabilities across a network to DataPower gateways
  - Remote HSM not supported for TLS/SSL use
  - Highly secure method for storing keys used by DataPower virtual instances



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

*Figure 9-19. Remote Hardware Security Module (HSM)*

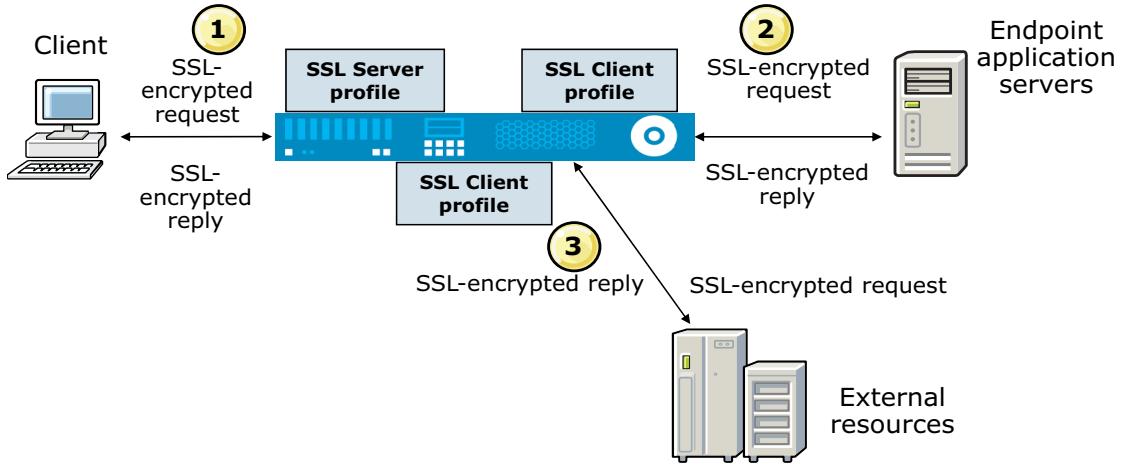
A remote Hardware Security Module (HSM) resides on a machine outside of the DataPower instance. This capability is useful for virtual gateways.

The remote HSM can store and deliver keys only. It is not possible to generate keys through the DataPower GUI currently.

## DataPower support for SSL

DataPower gateway supports TLS/SSL:

1. From remote client to gateway by using SSL Server profile
2. From gateway to external application server by using SSL Client profile
3. From gateway to external resource, such as authentication server, by using SSL Client profile



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-20. DataPower support for SSL

SSL is a point-to-point protocol. A new SSL connection is required for each point. For example, three separate SSL connections are required for connections from remote client to gateway, gateway to endpoint application server, and gateway to external resource.

## SSL profiles

The SSL profiles define the SSL properties of the different ends of the SSL session

- Both SSL profiles specify:
  - Supported SSL/TLS protocols
  - Supported RSA and ECDSA cipher suites
  - SSL session caching
- Unique to SSL *client* profile:
  - Use SNI
  - Validation credential to validate the SSL server certificate
  - Identification credential to support client authentication
- Unique to SSL *server* profile
  - Identification credential to send server certificate
  - Validation credential to validate client certificate when mutual authentication is specified
  - Does *not* support SNI

Figure 9-21. SSL profiles

You can control whether to enable Server Name Indication (SNI). When enabled, the client sends an SNI extension in the ClientHello message to the server with the DNS name that the client attempts to connect to. By default, SNI is enabled.

The SSL server profile object does not support SNI. For SNI server support, you must use the SSL SNI server profile object.

## SSL - crypto object relationships

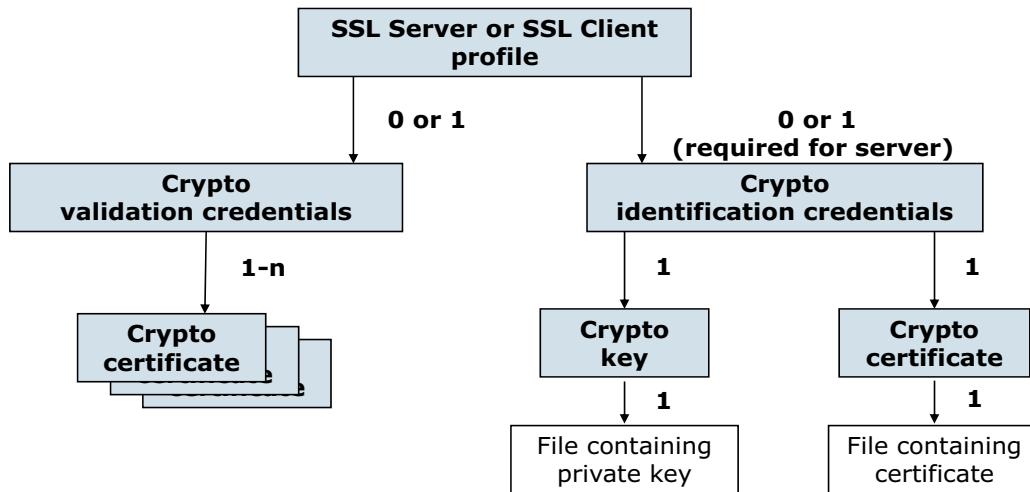


Figure 9-22. SSL - crypto object relationships

This graphic shows the relationships of the various objects and files that are involved in SSL and other crypto work on the gateway. An SSL Server profile object must have one Crypto identification credentials object associated with it. An SSL Client profile can optionally omit this association.

The crypto key and crypto certificate are also used in encryption and digital signatures.

**IBM Training**

**IBM**

## DataPower as the SSL server (from client to gateway) (1 of 2)

- To support SSL requests from the client:
  - A required **SSL Server profile** object links to ID credentials and specifies the cipher specifications that are allowed for the connection
  - DataPower gateway returns a cryptographic certificate to the client
  - The matching private key for the certificate indicated in the **ID credentials**

Name: DPEdu \*

**General**

Administrative state:  enabled  disabled

Comments: Exclude compromised protocols

Protocols:

- Enable SSL version 3
- Enable TLS version 1.0
- Enable TLS version 1.1
- Enable TLS version 1.2

Ciphers:

ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	↑ ↓ X
ECDHE_RSA_WITH_AES_256_GCM_SHA384	↑ ↓ X
ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	↑ ↓ X
ECDHE_RSA_WITH_AES_256_CBC_SHA384	↑ ↓ X

Identification credentials: DPEdu \* + ...

DataPower cryptographic tools and SSL setup © Copyright IBM Corporation 2018

Figure 9-23. DataPower as the SSL server (from client to gateway) (1 of 2)

As of version 7.5, DataPower uses new objects to implement SSL and TLS connections. The SSL Server profile implements the server side of such a connection.

## DataPower as the SSL server (from client to gateway) (2 of 2)

- The client can validate the certificate that the gateway presents, which is often included in certificate chain (server-only authentication)
  - Gateway can request a certificate from the client and validate client (mutual authentication)
  - Gateway uses certificates in the *validation credentials* that are identified in the SSL Server profile to validate the client certificate

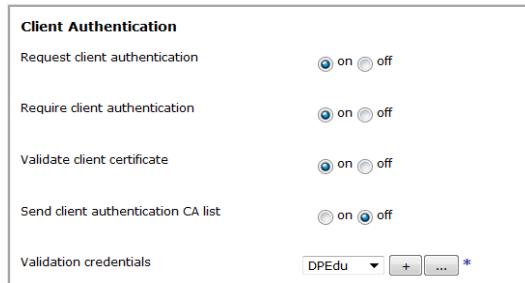


Figure 9-24. DataPower as the SSL server (from client to gateway) (2 of 2)

The server can request authentication credentials from the client; this situation is known as “mutual authentication.” The server then validates the certificate that is presented by the client by using a validation credential object.

## DataPower as the SSL client (from gateway to back-end server) (1 of 2)

- To set up SSL between the gateway and a remote server:
  - A required **SSL Client profile** object specifies the cipher specifications acceptable for the connection
  - Client uses hostname in target URL for SNI by default; this option can be turned off
  - Alternate SNI hostname can be used instead of default when SNI enabled

The screenshot shows the configuration interface for an SSL Client profile. It includes the following sections:

- Protocols:** Options to enable SSL version 3, TLS version 1.0, TLS version 1.1, and TLS version 1.2.
- Ciphers:** A list of available ciphers, including ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384, ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384, and ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384. The first two are selected.
- Features:** Options to use SNI, permit connections to insecure servers, and enable compression. The 'Use SNI' checkbox is checked.
- Use custom SNI Hostname:** A dropdown menu set to 'Yes' with an asterisk indicating it is required.
- Custom SNI hostname:** An input field containing 'EduServer' with an asterisk indicating it is required.

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-25. DataPower as the SSL client (from gateway to back-end server) (1 of 2)

An SSL Client can optionally send the SNI ‘clientHello’ TLS extension value to request connection to a particular hostname. If a Custom SNI hostname is given, this value is used instead of the hostname that was given in the target URL.

## DataPower as the SSL client (from gateway to back-end server (2 of 2))

- To set up SSL between the gateway and a remote server:
  - Client can validate server certificate by using optional **Validation credentials**
  - Client uses certificate that is specified in optional ID credentials to respond to server request for mutual authentication

The screenshot shows a configuration panel for an SSL client. At the top, 'Use custom SNI Hostname' is set to 'Yes'. Below it, 'Custom SNI hostname' is set to 'EduServer'. Under the 'Credential' section, 'Identification credentials' is set to 'DPEdu'. There is also a 'Validation credentials' section with 'DPEdu' selected. Under 'Validate server certificate', the 'on' radio button is selected. There are also '+' and '...' buttons for managing credentials.

*Figure 9-26. DataPower as the SSL client (from gateway to back-end server (2 of 2))*

The client uses the Identification credentials to respond to requests for mutual authentication by the SSL server.

## Securing connection from gateway to external resource server

To set up SSL between the gateway and external resource server:

- The gateway acts as a client and uses an **SSL Client profile**
- A User Agent object identifies the SSL Client profile to use based on the target URL

The resource server might request a certificate for the gateway (mutual authentication)

- Gateway can respond with the certificates in the **identification credentials**

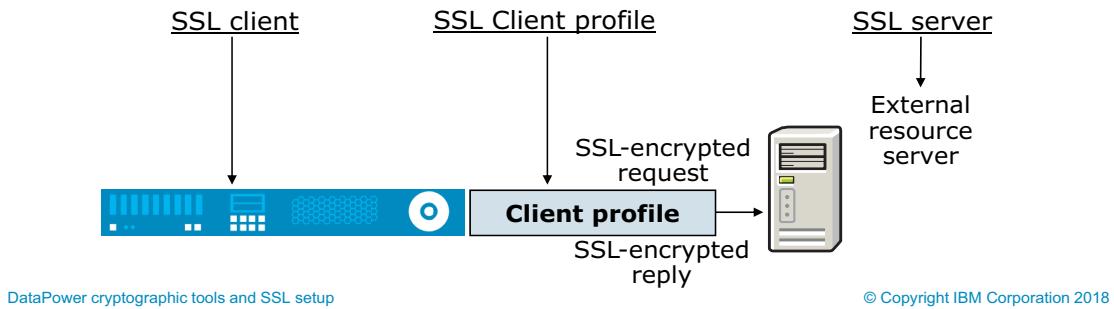
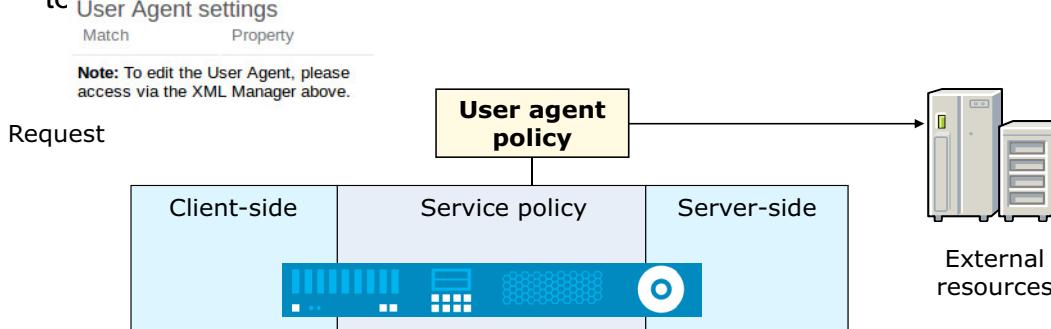


Figure 9-27. Securing connection from gateway to external resource server

The gateway uses the SSL Client profile to connect to any external server that requires SSL, such as an authentication server or database server.

## What is a “user agent”?

- The User Agent can be thought of as a utility object that other higher-level DataPower objects use
- *The User Agent primarily handles the details for network-related outbound calls from the gateway*
- The settings on the **SSL Profile Policy** of the User Agent apply to SSL connections from the gateway to remote targets
- The User Agent offers many other possible settings that are not related to User Agent settings



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-28. What is a “user agent”?

A **user agent** is a client that initiates a request for a local service to establish a connection to a remote server.

A user agent uses one or more policies to connect to an external server or back side service.

In the Blueprint Console, the user agent can be set from the XML Manager settings of a multi-protocol gateway.

## Configuring a user agent (1 of 2)

The User Agent is specified on the XML Manager main page

- The **default** XML manager object uses a **default** user agent
- Alternatively, from the vertical navigation bar, click **Network > Other > User Agent** to display or create a user agent

User Agent	Status: up
default	
* Name: default	
▾ Main	
Enable administrative state:	<input checked="" type="checkbox"/>
Comments:	Default User Agent
HTTP Request-Header:	
Maximum Redirects:	8
Timeout:	300
▶ Proxy Policy	
▶ SSL Profile Policy	
▶ Basic-Auth Policy	

Figure 9-29. Configuring a user agent (1 of 2)

The XML Manager in use by the service that requires a connection to a remote host using SSL identifies a User Agent object to use to manage those connections.

## Create a user agent configuration (2 of 2)

- Configure a user agent to use an SSL proxy profile to communicate with back-end service
  - Enter a name for the user agent object, if not reusing one
  - Click the **SSL Profile Policy** tab
  - Click **Add**
  - Specify a URL match expression ('\*' represents any value)
  - Set the SSL Client type to Client Profile
  - Select the required profile or click **New** to create one
  - Click **Apply**

The screenshot shows a configuration dialog for an SSL Profile Policy. The 'Name' field is filled with 'DPEdu'. Under the 'SSL Matching Expression' tab, the URL matching expression is set to '\*'. The 'SSL client type' is set to 'Client Profile'. In the 'SSL client profile' section, 'DPEdu' is selected from a dropdown, accompanied by a '+' button and an ellipsis button. The tabs at the top of the dialog are 'URL Matching Expression' (which is active and highlighted in blue), 'SSL proxy profile (deprecated)', 'SSL client type', and 'SSL client profile'.

DataPower cryptographic tools and SSL setup

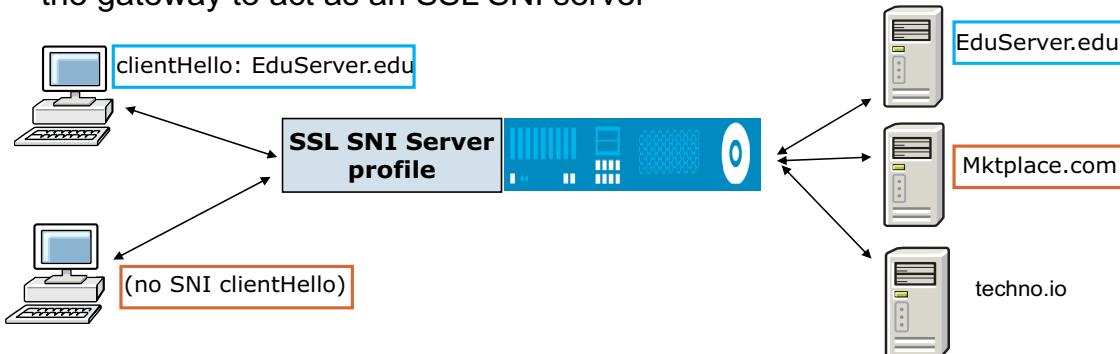
© Copyright IBM Corporation 2018

*Figure 9-30. Create a user agent configuration (2 of 2)*

The user agent employs a URL map to select the SSL Client profile to use.

## SSL SNI server profile (1 of 2)

- The Server Name Indication (SNI) extension to TLS allows an SSL server to support multiple certificates on the same IP address
  - Unique certificates can be served dependent on requested host name
- Client indicates requested host name during SSL handshake
  - SSL server returns certificate that matches that host name
- The SSL SNI server profile defines the configuration that is needed by the gateway to act as an SSL SNI server



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-31. SSL SNI server profile (1 of 2)

The SSL SNI Server profile is new in version 7.5.

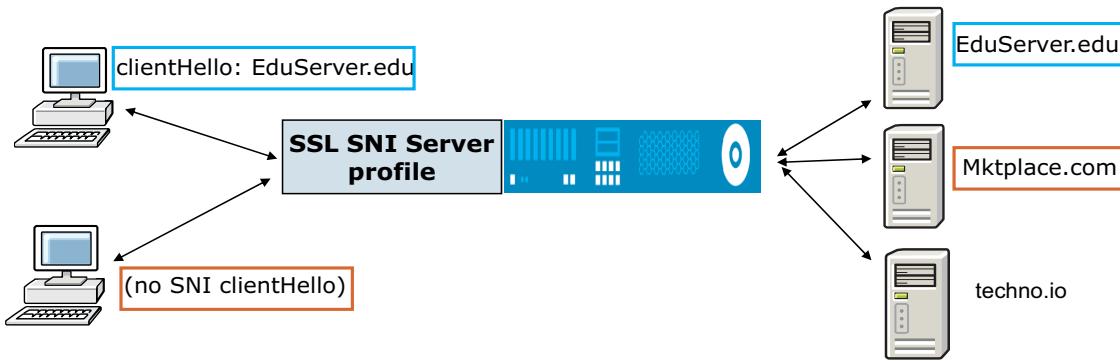
In the graphic, this gateway supports EduServer.edu, Mktplace.com, and techno.io on the same IP address.

The top client requests EduServer.edu, which DNS converts to the appropriate IP address. The client also included an SNI extension that contains "EduServer.edu". The SSL SNI server profile object detects the SNI extension, and returns the certificate for EduServer.edu.

The bottom client sends a request that does not include the SNI extension. What happens depends on the configuration of the SSL SNI server profile.

## SSL SNI server profile (2 of 2)

- The SSL SNI server profile refers to a Host Mapping object:
  - Maps host name that is requested by client to an SSL server profile
  - Each SSL server profile specifies its own certificate (identification credential)
  - Allows DataPower to proxy more than one hostname on single gateway
- A Default SSL Server profile can be specified to handle clients that do not send an SNI ‘clientHello’ request



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-32. SSL SNI server profile (2 of 2)

Note that when no Default SSL server profile is configured, the SSL SNI server rejects connection requests from clients that do not send an SNI ‘clientHello’ hostname in the connection request.

For the bottom client, if no default server profile is specified in the SSL SNI server profile, the request fails. In the example, the default server profile points to the Mktplace.com site, so the client is sent the certificate for that site.



## SSL Host Name Mapping

- The SSL Host Name Mapping maps requested hosts to SSL server profiles
- Access the SSL Host Name Mapping object from the SSL SNI server profile page or going to **Objects > Crypto Configuration > SSL Host Name Mapping**

SSL Host Name Mapping: MultiHostname [up]

[Apply](#) [Cancel](#) [Undo](#) [Export](#) | [View Log](#) | [View Status](#) | [Help](#)

Administrative state	<input checked="" type="radio"/> enabled <input type="radio"/> disabled																		
Comments	Falls to Mktplace if no other match																		
Host Name to SSL Server Profile Mapping	<table border="1"> <thead> <tr> <th>Host name matching expression</th> <th>SSL Server Profile</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>*EduServer.edu</td> <td>DPEdu</td> <td></td> </tr> <tr> <td>*Mktplace.com</td> <td>DPMktplace</td> <td></td> </tr> <tr> <td>*techo.io</td> <td>DPTechno</td> <td></td> </tr> <tr> <td>=</td> <td>DPMktplace</td> <td></td> </tr> <tr> <td>*</td> <td></td> <td><a href="#">Add</a></td> </tr> </tbody> </table>	Host name matching expression	SSL Server Profile	Actions	*EduServer.edu	DPEdu		*Mktplace.com	DPMktplace		*techo.io	DPTechno		=	DPMktplace		*		<a href="#">Add</a>
Host name matching expression	SSL Server Profile	Actions																	
*EduServer.edu	DPEdu																		
*Mktplace.com	DPMktplace																		
*techo.io	DPTechno																		
=	DPMktplace																		
*		<a href="#">Add</a>																	

DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-33. SSL Host Name Mapping

The SSL Host Name Mapping object examines the hostname sent by the client and attempts to match it to an SSL server profile. At least one entry in this map is required.

## The SSL proxy profile (deprecated)

- The SSL proxy profile specifies the SSL server and SSL client crypto profiles for a DataPower service
  - Can list 0, 1, or 2 crypto profiles
- The crypto profiles are designated as **forward** or **reverse**
  - **Reverse** is when the gateway or service is the SSL server
  - **Forward** is when the gateway or service is the SSL client
- Controls SSL session caching
- Specifies whether mutual authentication is required

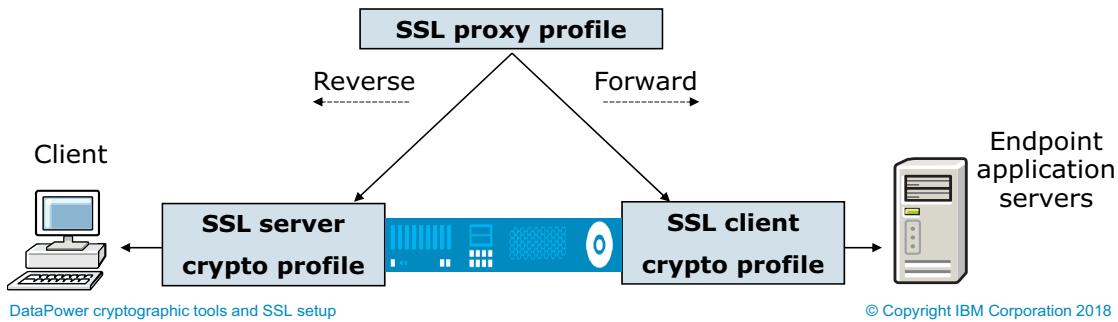


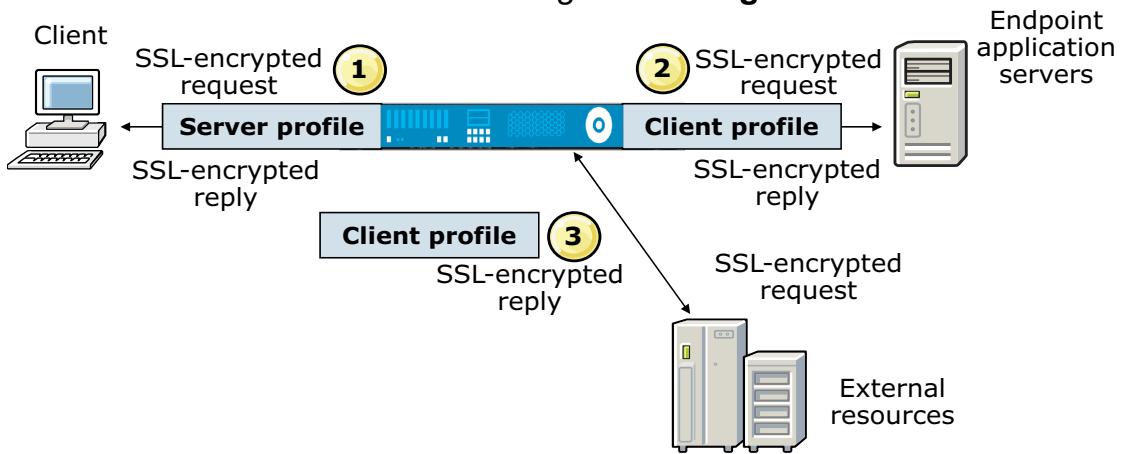
Figure 9-34. The SSL proxy profile (deprecated)

An SSL proxy profile uses a Crypto profile to implement the required security settings for SSL/TLS connections. A single SSL proxy profile can act as a server, a client or both, depending on the configuration of the Crypto profiles that are used.

The SSL proxy profile is deprecated. Support is offered for existing configurations.

## A crypto profile (deprecated) specifies details of the SSL connection

- It defines:
  - How much DataPower endpoint verification to do, and how to do it
  - What cipher specifications DataPower can use for this connection
- “1” and “2” are defined directly within the service specification
- “3” is defined within an XML Manager’s **user agent**



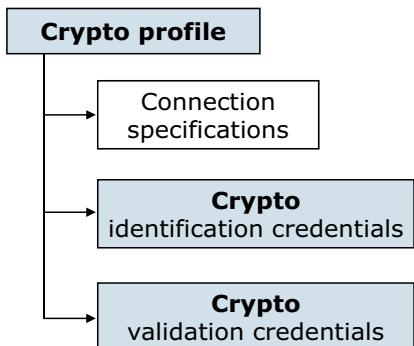
DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-35. A crypto profile (deprecated) specifies details of the SSL connection

## Crypto profile (deprecated)

- Specifies the DataPower end of the SSL connection
- Particulars depend on whether this profile is for an “SSL client” or an “SSL server” end of the connection



The screenshot shows the "Main" configuration page for a Crypto profile named "DPAdminSSLProfile". The "Name" field is set to "DPAdminSSLProfile". The "Enable administrative state" checkbox is checked. The "Identification Credentials" dropdown is set to "idcred-DPAdminSSLProfile". The "Validation Credentials" dropdown is empty. The "Ciphers" dropdown is set to "DEFAULT". In the "Options" section, several checkboxes are present: "Enable default settings" (checked), "Disable SSL version 2" (checked), "Disable SSL version 3" (unchecked), "Disable TLS version 1.0" (unchecked), and "Permit insecure SSL renegotiation to a legacy SSL client" (unchecked).

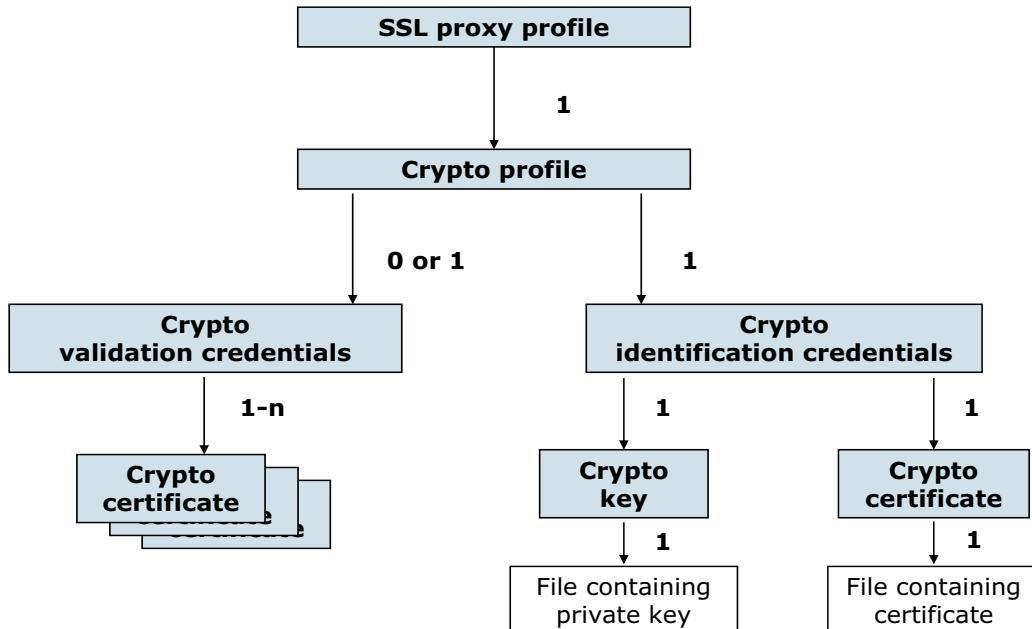
DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-36. *Crypto profile (deprecated)*

The **Ciphers** field specifies what cipher specifications are supported at the DataPower end of the connection. It is composed of one or more cipher suites.

## Proxy profile - crypto object relationships (deprecated)



DataPower cryptographic tools and SSL setup

© Copyright IBM Corporation 2018

Figure 9-37. Proxy profile - crypto object relationships (deprecated)

Numerous objects are involved in configuring legacy SSL support. This graphic provides an opportunity to review them.

## Unit summary

- Explain how to use the DataPower tools to generate cryptographic keys
- Create a cryptographic identification credential object that contains a matching public and private key
- Create a cryptographic validation credential to validate certificates
- Set up certificate monitoring to ensure that certificates are up-to-date
- Configure an SSL server profile that accepts an SSL connection request from a client
- Configure an SSL client profile that initiates an SSL connection from a DataPower service
- Configure an SSL SNI server profile that supports SNI requests

Figure 9-38. Unit summary

## Review questions (1 of 2)

1. What default configuration is provided with DataPower to notify administrator of a certificate expiration?
  - A. DataPower automatically renews expired certificates
  - B. Expired certificates are removed from the gateway and placed in the expired certificate directory
  - C. Certificates do not expire
  - D. Expired certificates are written to a log file with a specified warning
2. True or False: Keys that are generated onboard cannot be exported.



Figure 9-39. Review questions (1 of 2)

Write your answers here:

- 1.
- 2.

## Review questions (2 of 2)

3. True or False: When the remote client initiates an SSL session to a DataPower service, the service end is the “SSL server.”
  
4. True or False: DataPower cannot support clients that *do not* send SNI host name information and support clients that *do* send SNI host name information with the *same* SSL SNI Server profile.



Figure 9-40. Review questions (2 of 2)

Write your answers here:

- 3.
  
- 4.

## Review answers (1 of 2)

1. What default configuration is provided with DataPower to notify administrator of a certificate expiration?
  - A. DataPower automatically renews expired certificates
  - B. Expired certificates are removed from the gateway and placed in the expired certificate directory
  - C. Certificates do not expire
  - D. Expired certificates are written to a log file with a specified warning

The answer is D.

  
- 2. True or False: Keys that are generated onboard cannot be exported.  
The answer is False. Keys can be exported to the `temporary:` directory if the **Export Private Key** is selected when generating a key on the gateway.



Figure 9-41. Review answers (1 of 2)

## Review answers (2 of 2)



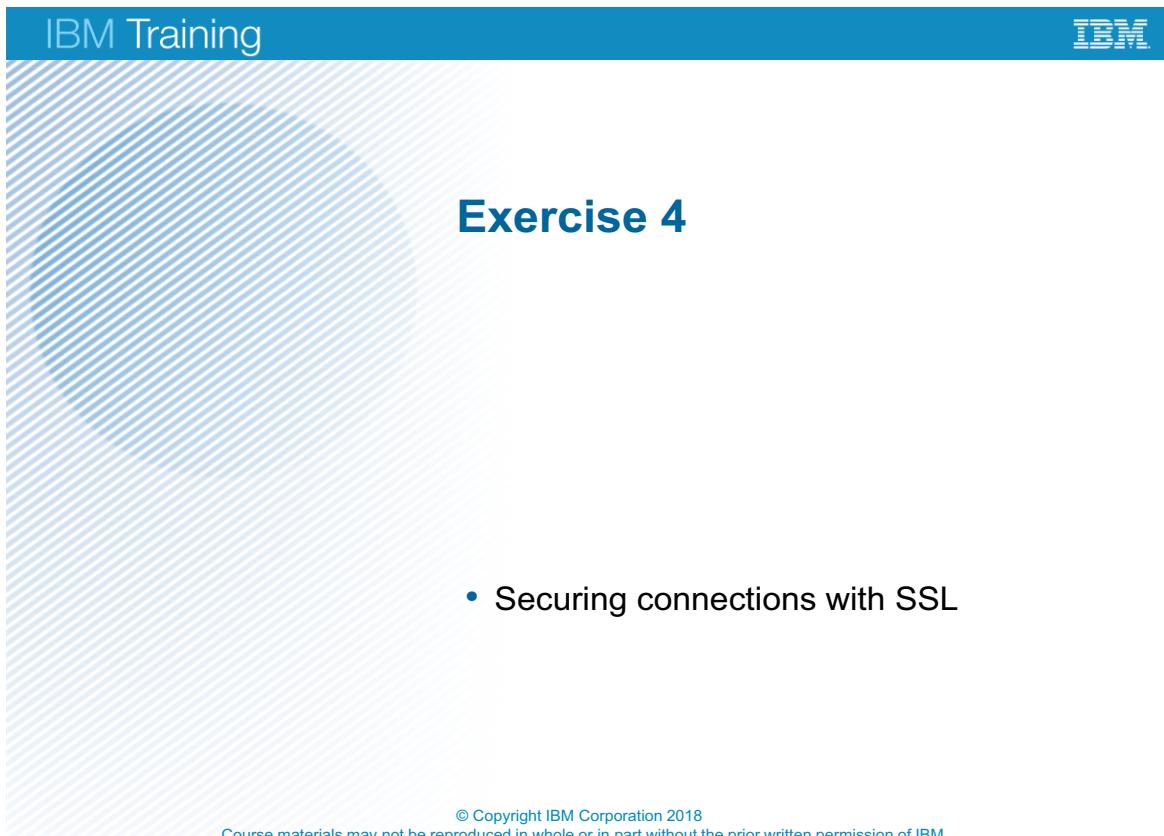
3. True or False: When the remote client initiates an SSL session to a DataPower service, the service end is the “SSL server.”

The answer is True.

4. True or False: DataPower cannot support clients that *do not* send SNI host name information and support clients that *do* send SNI host name information with the *same* SSL SNI Server profile.

The answer is False. The default server profile in the SSL SNI server profile supports SSL clients that do not send the SNI extension.

Figure 9-42. Review answers (2 of 2)



The slide is titled "Exercise 4" in large blue text at the top right. The background features a light gray diagonal striped pattern. A blue header bar at the top left contains the text "IBM Training". A blue footer bar at the bottom contains copyright information.

**Exercise 4**

- Securing connections with SSL

© Copyright IBM Corporation 2018  
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Figure 9-43. Exercise 4

## Exercise objectives

After completing this exercise, you should be able to:

- Use the DataPower cryptographic tools to generate cryptographic keys
- Use a cryptographic key and certificate object to create a cryptographic identification credential
- Use a validation credential object to validate certificates
- Create an SSL proxy profile to accept SSL connections from a client

Figure 9-44. Exercise objectives

## Exercise overview (1 of 2)

- Create the files and objects that are needed to configure the SSL connections for the services



Figure 9-45. Exercise overview (1 of 2)

## Exercise overview (2 of 2)

- Verify that the SSL connection is using the new “StudentKeyObj” certificate

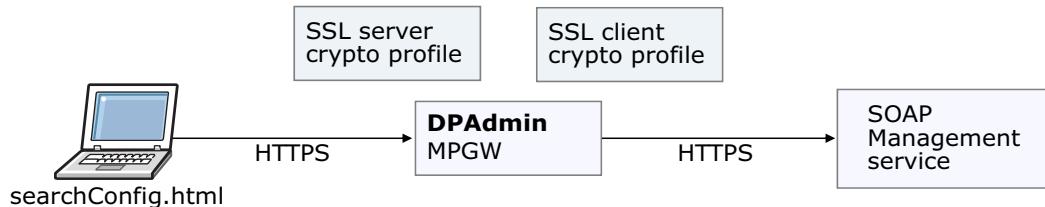


Figure 9-46. Exercise overview (2 of 2)

# Unit 10. Logging and log targets

## Estimated time

00:30

## Overview

This unit shows you how to capture information that can be generated by DataPower events by using the logging utilities, such as the log target and log action. You learn how to configure a log target to limit the messages to specific severities, categories, and event codes. You also learn how to send log messages off the box to a remote system. Finally, the unit describes SNMP support within the appliance.

## How you will check your progress

- Review questions
- Lab exercise

## References

## Unit objectives

- Describe the publish/subscribe model of log targets and log events
- Define log levels, event categories, and event codes
- Create a log category to capture messages that objects on the appliance generate
- Generate a test message for the log category

Figure 10-1. Unit objectives

## Logging on the DataPower Gateway

Capture and “saving” of real-time information:

- The “saving” can be to a local file, remote server, or through email

Function of logging:

- Operational
  - Remote server cannot be reached
  - Authentication failed
  - Resources changed
- Application
  - Capture message data
  - Specific application situation (event) occurs that needs to be noted, such as a message that contains data that crosses some application threshold

**Log targets** handle appliance or application events.

Capturing of message data is done by using a **log action** in a service processing policy.

Figure 10-2. Logging on the DataPower Gateway

The function of logging can be:

Operational:

- Remote server cannot be reached
- Authentication failed
- Resources changed

Application:

- Capture message data
- Specific application situation (event) occurs that needs to be noted, such as a message that contains data that crosses some application threshold.

## Logging basics

- Logging system is based on the publish/subscribe model
  - Objects *publish* events
  - Subscribers *subscribe* to events of interest
- The DataPower logging system uses **log targets** as *subscribers* and **log events** (generated by objects) as *publishers*
- Logs can be written on-device or off-device
  - On-device logs can be moved off-device (SFTP, SCP, HTTP, HTTPS)
  - Off-device support for syslog, syslog-tcp, SNMP
- Log targets do not capture the actual message
  - Add a **Log** action in a processing rule to capture the entire message

Figure 10-3. Logging basics

Log files can be encrypted or signed for more security.

Objects that generate log messages have different priorities. These messages range from verbose debugging to infrequent critical or emergency level messages.

Log targets are subscribers that subscribe to logging events. Logging events are called log categories in the DataPower terminology. Service components, such as an MPGW, emit, or publish events, that are based on the document processing that they do. Other system components also generate or publish events.

Log messages get sent to log targets that are based on the events for which a log target subscribes. In addition, the message that gets logged also depends on the logging level.

## Available log levels

Log level indicates the severity of an event:

- **emergency**: System is unusable
- **alert**: Immediate action must be taken
- **critical**: Critical condition
- **error**: An error occurred and the error code is included
- **warning**: A warning condition occurred
  - Nothing is wrong, but conditions indicate that a problem can occur soon if nothing changes
- **notice**: A normal but significant condition applies
- **information**: Only an informational message
- **debug**: Debug-level messages
  - This level generates numerous messages

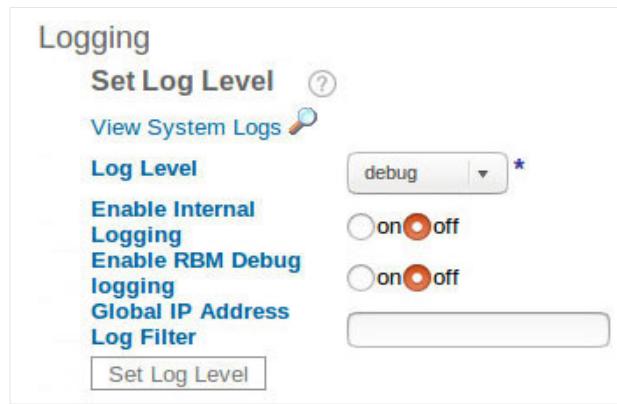


Figure 10-4. Available log levels

The default system log is set up as a log target that subscribes to all events that the appliance generates.

Log targets capture messages at or above the configured level.

This input sets the level at which the default system log captures messages. It is accessed from the Administration icon. Then, select **Debug> Troubleshooting**.

You can increase the amount of logging information by enabling internal logging and RBM debugging.

IBM Training 

## Event categories

- Functional area with categorized event messages
- Administration > Miscellaneous > Configure Log Categories**
  - Note the **all** category, which indicates no filtering by category
- You can add your own categories
  - Custom categories must be unique across all domains

Name	Status	Op-State	Comments	Actions
aaa	saved	up	AAA Policy	 
all	saved	up	All Categories	 
apiconnect	saved	up	API Connect	 
audit	saved	up	Audit Trace	 
auth	saved	up	Authentication	 

Figure 10-5. Event categories

## Event codes (1 of 2)

- Each event message has a code
  - **Administration > Debug > View List of Event Codes**

Event Code	Category	Severity	Message
0x02c60001	audit	info	Configuration settings applied
0x02c60002	audit	info	Configuration added
0x02c60003	audit	info	Configuration deleted
0x02c60004	audit	info	Password changed
0x02c30005	audit	error	Maximum number of failed logins.
0x02c60006	audit	info	admin-state disabled.
0x02c60007	audit	info	admin-state enabled.
0x02c30008	audit	error	Lock out due to number of failed logins

Figure 10-6. Event codes (1 of 2)

The diagram shows some event codes and lists typical events that are monitored.

## Event codes (2 of 2)

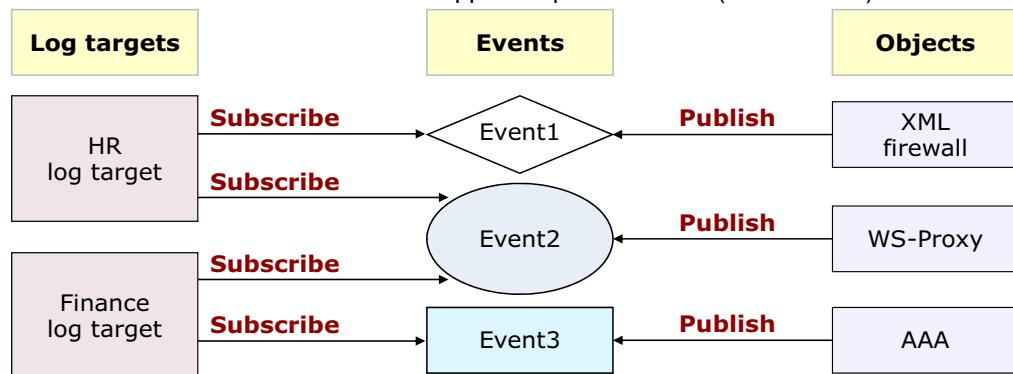
- Typical “critical” events that **are** monitored:

Event code	Category	Severity	Message
0x02210001	environmental	critical	Power supply failure
0x02210003	environmental	critical	Internal cooling fan is stopped
0x01a40001	system	warning	Throttling connections because of low memory
0x01a30002	system	error	Restart because of low memory
0x01a40005	system	warning	Throttling connections because of low temporary file space
0x01a40008	system	warning	Throttling connections because of low number of free ports
0x01a1000e	system	critical	Installed battery is nearing end of life
0x01a30015	system	error	Out of memory

Figure 10-7. Event codes (2 of 2)

## Log targets

- Log targets subscribe to log messages posted by the various running objects
  - Create a log target by selecting **Administration > Miscellaneous > Manage Log Targets**
- Restrictions on log target subscriptions:
  - Event subscription: Events generate at a minimum log level within specific categories
  - Object filters: Events specific to an instance of an object
  - Event filter: Can subscribe to or suppress specific events (event codes)



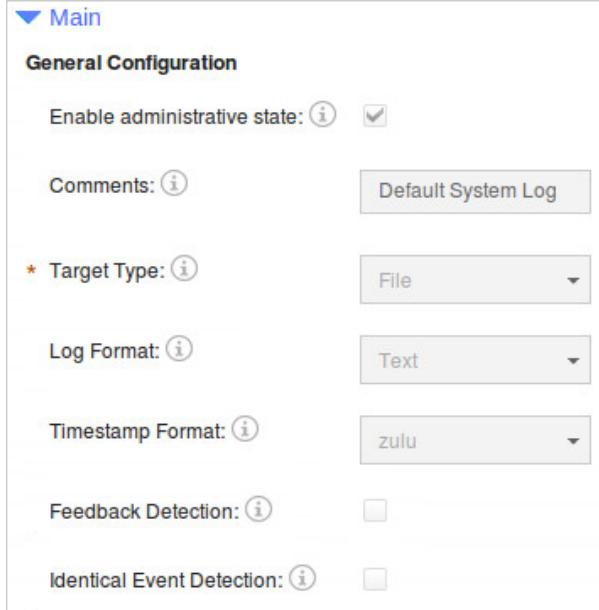
Logging and log targets

© Copyright IBM Corporation 2018

Figure 10-8. Log targets

The diagram in the slide shows 2 log targets: HR and Finance log targets. These log targets subscribe to certain types of events that are generated or published from objects on the DataPower gateway.

Use the Generate Log Event tool in the Troubleshooting pane to test whether log targets capture the log messages.



The screenshot shows the 'Manage Log targets: Main' configuration page. It has a header with 'IBM Training' and the IBM logo. The main section is titled 'General Configuration' under a 'Main' category. It includes fields for 'Enable administrative state' (checked), 'Comments' (empty), 'Target Type' (set to 'File'), 'Log Format' (set to 'Text'), 'Timestamp Format' (set to 'zulu'), 'Feedback Detection' (unchecked), and 'Identical Event Detection' (unchecked). The footer contains links for 'Logging and log targets' and 'Copyright IBM Corporation 2018'.

### Configuring a log target

- Use expandable menus to customize what events are captured
- **Log format** specifies data format of log entry
- **Feedback detection** ignores events from the logging subsystem itself
- **Identical event detection** suppresses events from the same object over a specified time period

Figure 10-9. Manage Log targets: Main

In the Blueprint Console, select the Administration icon. Then, select **Miscellaneous > Manage Log Targets**. Click the log target object to open the configuration page.

Log targets capture messages that are posted from the various objects and services that are running on the gateway. **Target types** enable more capabilities that include rotating files, encrypting and signing files or messages, and sending files to remote servers.

**Log Format** specifies the format in which to represent log entries:

- Text: Events as formatted text
- Raw: Events as unformatted text
- XML: Events in XML format
- CBE: Events in IBM Common Base Event format
- CSV: Events in comma-separated value (CSV) format

**Timestamp Format** specifies the format of the timestamp for log entries:

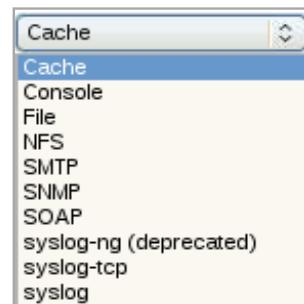
- Syslog: Uses the syslog-style timestamp
- Numeric: Uses a numeric timestamp

- Zulu: Milliseconds used as the timestamp format in Coordinated Universal Time (UTC) in log messages yyyyymmddThhmmss+oo:oo

## Log target types

A **Target Type** field supports the following values:

- **Cache**: Writes log entries to system memory
- **Console**: Writes log entries to a Telnet, SSH, or CLI screen on the serial port
- **File**: Writes log entries to a file on the gateway
- **NFS**: Writes log entries to a file on a remote NFS server
- **SMTP**: Forwards log entries as an email to configured addresses
- **SNMP**: Forwards log entries as SNMP traps
- **SOAP**: Forwards log entries as SOAP messages
- **syslog-*ng* (deprecated)**: Use syslog-tcp
- **syslog-tcp**: Uses TCP to forward log entries to a remote syslog daemon
  - The local address, remote address, remote port, syslog facility can be set
  - An SSL connection to the syslog host can be created
  - The processing rate can be limited
- **syslog**: Forwards log entries to a remote syslog daemon over UDP



[Logging and log targets](#)

© Copyright IBM Corporation 2018

Figure 10-10. Log target types

The log entries that are stored on a **local** or **NFS** file can be rotated, emailed, or uploaded to other locations. The entire file can also be encrypted and signed.

SNMP is a network protocol that allows for the exchange of management information between network devices. This protocol is included in the TCP/IP protocol suite.

Syslog is the format and protocol that is used to send messages over TCP or UDP to a Syslog daemon (syslogd). It allows for log messages to be collected from many applications.

Syslog-*ng* (New Generation) is deprecated. Use syslog-tcp instead.

Other fields might appear on the page dependent on the type of target that is selected.

## Manage Log targets: Event filters

- Event filters create filters for a log target that are based on *event codes*
  - Use the **Event Subscription Filter** to subscribe to specific event codes
  - Use the **Event Suppression Filter** to exclude certain event codes from being written to the log target
  - Click the **Select Code** button to add event codes to **Event Code** value list

Event Code	Category	Severity	Message
0x01530001	clock	error	Time zone config mismatch.
0x01b10001	crypto	alert	Crypto accelerator not supported by this
0x01b20002	crypto	critical	HSM is uninitialized
0x01b20003	crypto	critical	HSM PED login timed out
0x01b20004	crypto	critical	HSM PED login failed
0x01b10005	crypto	alert	Microcode file not found
0x01b10006	crypto	alert	Microcode load failed
0x01b10007	crypto	alert	HSM credentials not found
0x01b20008	crypto	critical	HSM password login failed

The screenshot shows the 'Event Filters' configuration screen. It contains two main sections: 'Event Subscription Filter' and 'Event Suppression Filter'. Each section includes a status message ('No items.'), an 'Add' button, and a 'Select Code' button. The 'Select Code' buttons in both sections are highlighted with a red box, indicating they are the focus of the instructions.

Logging and log targets

© Copyright IBM Corporation 2018

Figure 10-11. Manage Log targets: Event filters

You can subscribe the current log target to particular event code. Example event codes include out of memory, failed to install on local port, and other codes.

These event codes are event conditions that are specific to DataPower.

## Manage Log targets: Object filters

- Object filters allow only those messages that the selected objects generate to be written to a log target
- It is possible to create a log target that collects log messages for a particular class of objects
  - Example: AAA policy object called MyTest

**▼ Object Filters**

Object Filters: <a href="#">i</a>	
* Object Type: <a href="#">i</a>	AAA Policy
* Object Name: <a href="#">i</a>	MyTest
Add Referenced Objects: <a href="#">i</a>	<input type="checkbox"/>

Figure 10-12. Manage Log targets: Object filters

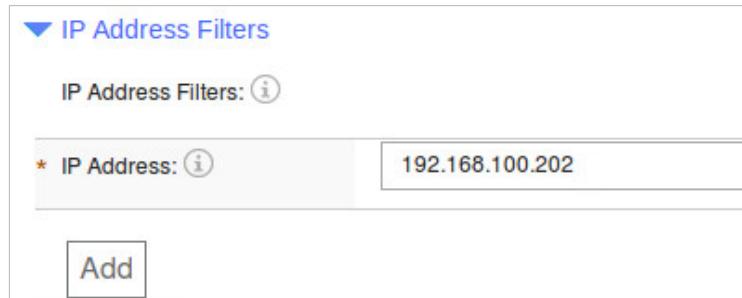
The object filter is more specific than the object class name. This filter collects log messages of an instance of a class.

For example, a log target would collect messages from an MPGW that is named MyMPGW and not all MPGW instances.

It is possible to create a log target that collects log messages from a particular class of objects only, such as a AAA policy. It is important to recognize that by using this filtering framework, you can design a sophisticated logging subsystem in which log targets are well-segregated to record specific events of interest.

## Manage Log targets: IP address filters

- IP address filters allow only those messages that originate from specified IP addresses to be written to a log target



The screenshot shows a user interface for managing log targets. At the top, there is a section titled "IP Address Filters" with a blue downward arrow icon. Below this, there is a label "IP Address Filters:" followed by a help icon. A table row contains a field labeled "IP Address:" with a required asterisk (\*) and a value "192.168.100.202". At the bottom of the table row is a blue "Add" button.

Figure 10-13. Manage Log targets: IP address filters

An IP address filter can log messages that come only from a specific IP address.

## Manage Log targets: Event trigger

- Triggers the execution of one or more CLI commands when specified criteria are met
- Message ID: Message ID that triggers the command
- Regular expression: Regular expression that must match the message body to trigger the command
- Only once: When **on**, indicates that the command is triggered only the first time that the trigger criteria are met
- Only this trigger: When **on**, this command is triggered, but other commands that the same message ID triggers are not

**Event Triggers**

Event Triggers: <a href="#">?</a>	
* Message ID: <a href="#">?</a>	0x01230002
Regular Expression: <input type="text"/>	
* Only Once: <a href="#">?</a>	<input checked="" type="checkbox"/>
* Only this Trigger: <a href="#">?</a>	<input checked="" type="checkbox"/>
* CLI Command: <a href="#">?</a>	<input type="button" value="save error-report"/>

Figure 10-14. Manage Log targets: Event trigger

If there are multiple commands, semicolons must separate them.

This event trigger indicates that if an out-of-memory event occurs, a “save error-report” CLI command is issued only once.

## Manage Log targets: Event subscriptions

- Log targets subscribe to particular event categories
- Example event categories:
  - **mgmt**: For configuration management events
  - **system**: For appliance system events
  - **all**: For all events

- A priority level can be specified for each event category that is chosen
  - Another level of filtering

**Event Subscriptions**

Event Subscriptions:	
* Event Category:	mgmt
Minimum Event Priority:	notice
* Event Category:	system
Minimum Event Priority:	notice
* Event Category:	all
Minimum Event Priority:	debug

Figure 10-15. Manage Log targets: Event subscriptions

*Event categories* is the same term that is used to describe an object class name.

At least one event category must be defined for a log target to capture messages.

The “all” event category means that events are captured regardless of the category from which they come.



## Example: Create a log category

**Log Category**

<input checked="" type="checkbox"/> Log Category orderEntry03 *	<p>* Name: <input type="text" value="orderEntry03"/></p> <p>▼ Main</p> <p>Enable administrative state: <input checked="" type="checkbox"/></p> <p>Comments: <input type="text" value="messages related to orderEntry03"/></p> <p style="text-align: right;"><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
--------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 10-16. Example: Create a log category

### 1+1=2 Example

Sign on to the Blueprint Console your student domain with your student user.

Select Administration > **Miscellaneous > Configure Log Categories**.

Click **New** to create a log category.

Type orderEntry in the category name, and ensure that the administrative state is set to enabled.

Click **Apply**.



## Example: Display the log category

- Type the name of the category in the filter

Name	Status	Op-State	Comments	Actions
<input type="checkbox"/> orderEntry03	new	up	messages related to orderEntry03	

Figure 10-17. Example: Display the log category

---

### 1+1=2 Example

From the Administration > **Miscellaneous > Configure Log Categories**, type the name of the newly-created Log category in the filter.

The category is displayed in the list.

---

## Example: Generate a Log event

- Ensure that the Log Level is set to the same level or higher that is specified in the Logging area

The screenshot shows the 'Generate Log Event' dialog box. It has fields for Log Category (set to 'orderEntry03'), Log Level (set to 'error'), Log Message ('TEST msg - orderEntry03'), and Event Code (empty). A red box highlights the 'Generate Log Event' button at the bottom. Below the dialog is a confirmation message box with a warning icon, the text 'Generate log event of type 'orderEntry03', priority 'error', and message 'TEST msg - orderEntry03''? and two buttons: 'Confirm' and 'Cancel'.

Logging and log targets

© Copyright IBM Corporation 2018

Figure 10-18. Example: Generate a Log event

### 1+1=2 Example

From the Administration > **Debug > Troubleshooting**, go to the Generate Log Event area. Select the category that you created in the Log Category drop-down. Change the Log Level to the log level or higher that is set in the Logging area. Type a log message. Click the Generate Log Event.



## Example: View the event in the system log

Target:	default-log	Filter:	orderEntry03	(none)			
time	category	level	tid	direction	client	msgid	message
Apr 19, 2018 6:45:50 PM							
Thursday, April 19, 2018							
6:45:23 PM	orderEntry03	error					TEST msg - orderEntry03

Figure 10-19. Example: View the event in the system log

View the system log, and filter the log by the log category to display the generated message.

## Application-specific logging: Audit log

- Displays the changes to the configuration of the appliance and files that are stored on the appliance
- Viewable by using either:
  - WebGUI: Status > View Logs > Audit Log
  - CLI: `show audit-log`
- Stored in `audit:` Directory in the default domain
- Can be copied off-box:
  - Copy `audit:audit-log mailto:jb@smtp.we.ibm.com` (SMTP protocol)
  - Send file `audit:audit-log mail-server email-address`

```
20180419T202708.380Z [conf] [success] [0x8240001f]
 (student03@student03_domain:web-gui:192.168.100.200): (config-crypto)#
 certificate idcred-DPAdminSSLProfile_cert cert:///Alice-sscert.pem
20180419T202818.187Z [conf] [success] [0x82400022]
 (student03@student03_domain:web-gui:192.168.100.200): (config key idcred-
 DPAdminSSLProfile_key)#
 key idcred-DPAdminSSLProfile_key cert:///Alice-
 privkey.pem
20180419T202818.188Z [conf] [success] [0x8240001c]
 (student03@student03_domain:web-gui:192.168.100.200): key 'idcred-
 DPAdminSSLProfile_key' - Configuration added
```

Figure 10-20. Application-specific logging: Audit log

The audit log is not visible in the File Management that is available in the Web Management service.

The audit log is displayed in the browser with this address:

`https://<dp_internal_ip>:9090/system/dpViewer/audit?filename=audit:/audit-log`

You cannot copy anything to the `audit:` directory.

The `save error-report` and `send error-report` CLI commands include the audit log in the report.

## Unit summary

- Describe the publish/subscribe model of log targets and log events
- Define log levels, event categories, and event codes
- Create a log category to capture messages that objects on the appliance generate
- Generate a test message for the log category

Figure 10-21. Unit summary

## Review questions

- 1. True or False:** To test a Log Event, one would use the Generate Log Event option in the troubleshooting page to generate a log message, and verify that it is included or excluded in a log target.
- 2. True or False:** When creating a log target, it automatically subscribes to all events.

Figure 10-22. Review questions

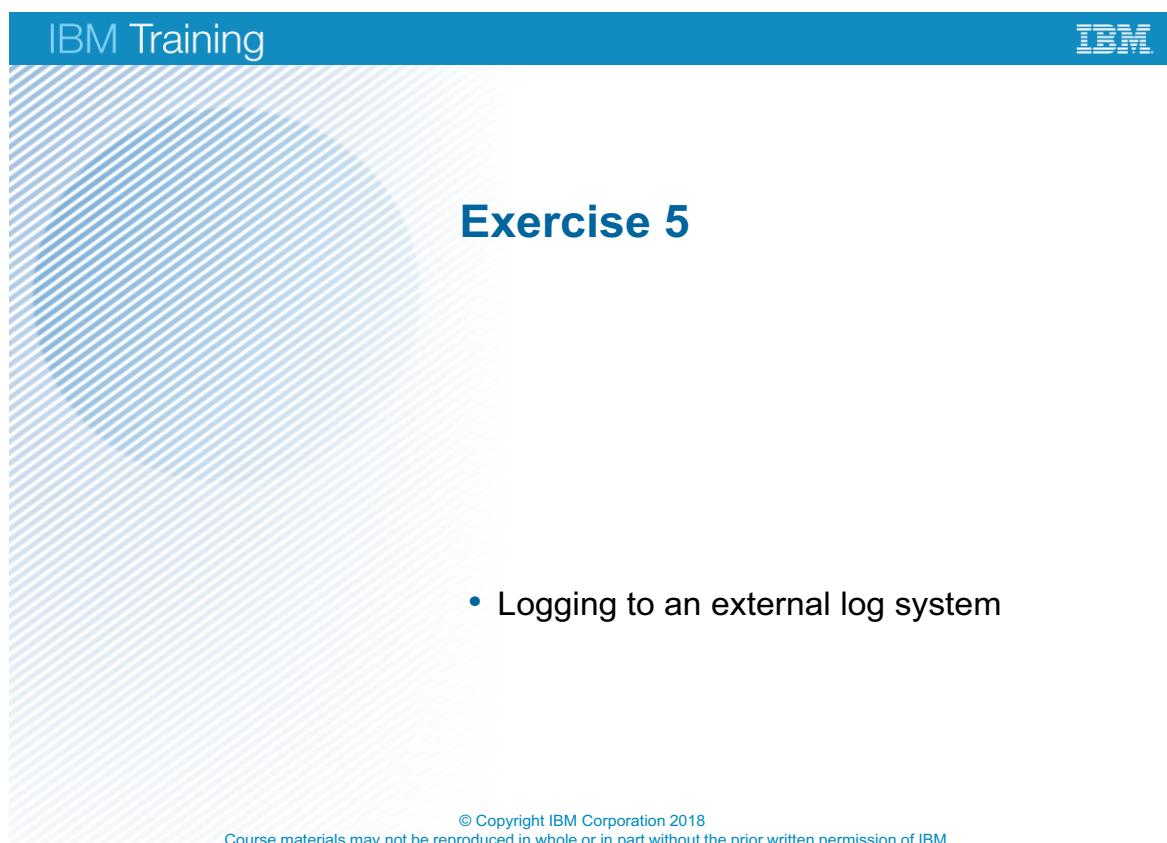
Write your answers here:

- 1.
- 2.

## Review answers

1. **True.** To test a Log Event, one would use the Generate Log Event option in the troubleshooting page to generate a log message, and verify that it is included or excluded in a log target.
2. **False.** A log target must subscribe to at least one event. The “all” category specifies that messages are logged for all categories.

Figure 10-23. Review answers



The slide features a blue header bar with 'IBM Training' on the left and the IBM logo on the right. Below the header is a large, light blue diagonal striped background area. In the center of this area, the text 'Exercise 5' is displayed in a bold, dark blue font. At the bottom of the slide, there is a copyright notice: '© Copyright IBM Corporation 2018' followed by a smaller line: 'Course materials may not be reproduced in whole or in part without the prior written permission of IBM.'

- Logging to an external log system

Figure 10-24. Exercise 5

## Exercise objectives

After completing this exercise, you should be able to:

- Use the Generate Log Event action to test the log target configuration
- Create a log target that subscribes to specific log categories
- Create a log target that sends log messages to an external logging system

Figure 10-25. Exercise objectives

---

# Unit 11. Course summary

## Estimated time

00:05

## Overview

This unit summarizes the course and provides information for future study.

## Unit objectives

- Explain how the course met its learning objectives
- Access the IBM Training website
- Identify other IBM Training courses that are related to this topic
- Locate appropriate resources for further study

Course summary

© Copyright IBM Corporation 2018

*Figure 11-1. Unit objectives*

## Course objectives

- Configure an appliance for its initial deployment
- Download and upgrade the firmware on the DataPower appliances
- Create and manage user accounts, groups, and domains
- Configure Secure Sockets Layer (SSL) to and from DataPower Appliances
- Troubleshoot and debug services by using the problem determination tools, logs, and probes that are provided with the DataPower appliance
- Configure logging of messages to external locations

Course summary

© Copyright IBM Corporation 2018

*Figure 11-2. Course objectives*

## Lab exercise solutions

- Solutions are available in the subdirectory:  
`<labfiles>/Solutions`

Remember to change:

- Port numbers
- IP addresses

Course summary

© Copyright IBM Corporation 2018

Figure 11-3. Lab exercise solutions

## To learn more on the subject

- IBM Training website:
  - <http://www.ibm.com/training>
  - Search on “DataPower training path”
- DataPower IBM Knowledge Center
  - [http://www.ibm.com/support/knowledgecenter/SS9H2Y\\_7.6.0](http://www.ibm.com/support/knowledgecenter/SS9H2Y_7.6.0)
- IBM Redbooks:
  - <http://www.redbooks.ibm.com>
  - Search on “DataPower”
- developerWorks articles:
  - <http://www.ibm.com/developerworks/>
  - Search on “DataPower”

Course summary

© Copyright IBM Corporation 2018

Figure 11-4. To learn more on the subject

## Unit summary

- Explain how the course met its learning objectives
- Access the IBM Training website
- Identify other IBM Training courses that are related to this topic
- Locate appropriate resources for further study

Course summary

© Copyright IBM Corporation 2018

*Figure 11-5. Unit summary*

# Appendix A. List of abbreviations

## A

<b>AAA</b>	authentication, authorization, and auditing
<b>AC</b>	alternating current
<b>ACL</b>	access control list
<b>ADT</b>	Android Development Tools
<b>AES</b>	Advanced Encryption Standard
<b>AMP</b>	Appliance Management Protocol
<b>Ant</b>	Another neat tool
<b>AO</b>	Application Optimization
<b>API</b>	application programming interface
<b>ARP</b>	Address Resolution Protocol
<b>ASCII</b>	American Standard Code for Information Interchange

## B

<b>B2B</b>	business-to-business
<b>B2C</b>	business-to-consumer

## C

<b>CA</b>	Certificate authority
<b>CBR</b>	content based routing
<b>CD ROM</b>	Compact Disk Read Only Memory
<b>CFG</b>	configuration
<b>CGI</b>	CGI Common Gateway Interface
<b>cHTML</b>	Compact HTML
<b>CIDR</b>	Classless Inter-Domain Routing
<b>cKVM</b>	Concurrent Keyboard, Video, and Mouse
<b>CLI</b>	command-line interface
<b>CN</b>	common name
<b>CPU</b>	central processing unit
<b>CR</b>	carriage return
<b>CRL</b>	certificate revocation list

<b>CSR</b>	certificate signing request
<b>CSR</b>	certificate signing request
<b>CSS</b>	cascading style sheet

**D**

<b>DAP</b>	Directory Access Protocol
<b>DB</b>	database
<b>DCO</b>	Database Connectivity Option
<b>DES</b>	Data Encryption Standard
<b>DH</b>	Diffie-Hellman
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DIME</b>	Direct Internet Message Encapsulation
<b>DIT</b>	directory information tree
<b>DMZ</b>	demilitarized zone
<b>DN</b>	distinguished name
<b>DNS</b>	domain name server
<b>DOM</b>	Document Object Model
<b>DOP</b>	data-oriented programming
<b>DoS</b>	denial-of-service
<b>DSS</b>	Digital Signature Standard
<b>DTD</b>	document type definition

**E**

<b>EDIINT</b>	Electronic Data Interchange-Internet Integration
<b>EMS</b>	Enterprise Message Service
<b>EMS</b>	Enterprise Messaging System
<b>EON</b>	Edge of Network
<b>ESB</b>	enterprise service bus
<b>ESR</b>	Extended Support Release
<b>EULA</b>	end-user license agreement
<b>EXSLT</b>	Extensions to Extensible Stylesheet Language Transformation

**F**

<b>FIFO</b>	first-in first-out
<b>FIPS</b>	Federal Information Processing Standard

<b>FIX</b>	Financial Information Exchange
<b>FO</b>	formatting object
<b>FTP</b>	File Transfer Protocol
<b>FTPS</b>	FTP over SSL

**G**

<b>GB</b>	gigabyte
<b>GSS</b>	Generic Security Services
<b>GUI</b>	Graphical user interface

**H**

<b>HR</b>	human resources
<b>HREF</b>	hypertext reference
<b>HSM</b>	hardware security module
<b>HSRP</b>	Hot Standby Router Protocol
<b>HTML</b>	Hypertext Markup Language
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	HTTP over SSL

**I**

<b>ICAP</b>	Internet Content Adaptation Protocol
<b>ICMP</b>	Internet Control Message Protocol
<b>IDE</b>	Integrated development environment
<b>IDEA</b>	International Data Encryption Algorithm
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IETF</b>	Internet Engineering Task Force
<b>ILD</b>	intelligent load distribution
<b>IM</b>	Intelligent Management
<b>IMM</b>	Integrated Management Module
<b>IMS</b>	Information Management System
<b>IP</b>	Internet Protocol
<b>IPMI</b>	Intelligent Platform Management Interface
<b>IPSec</b>	IP Security
<b>iSCSI</b>	Internet Small Computer Systems Interface
<b>ISO</b>	International Organization for Standardization

**J**

<b>JAXP</b>	Java API for XML Parsing
<b>JAXP</b>	Java API for XML Processing
<b>JDBC</b>	Java Database Connectivity
<b>JKS</b>	Java Key Store
<b>JMS</b>	Java Message Service
<b>JRE</b>	Java runtime environment

**K**

<b>KB</b>	kilobyte
<b>KVM</b>	Keyboard, Video, and Mouse

**L**

<b>LACP</b>	Link Aggregation Control Protocol
<b>LAN</b>	Local area network
<b>LCD</b>	liquid crystal display
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LDIF</b>	LDAP Data Interchange Format
<b>LED</b>	light-emitting diode
<b>LLM</b>	Low Latency Messaging

**M**

<b>MAC</b>	message authentication code
<b>MB</b>	megabyte
<b>MDB</b>	message-driven bean
<b>MFA</b>	message filter action
<b>MIB</b>	Management Information Base
<b>MIME</b>	Multipurpose Internet Mail Extensions
<b>MM</b>	message monitor
<b>MMXDoS</b>	Multiple message XML denial-of-service
<b>MPG</b>	multi-protocol gateway
<b>MPGW</b>	multi-protocol gateway
<b>MQ</b>	Message Queue
<b>MQFTE</b>	MQ File Transfer Edition

<b>MT</b>	message type
<b>MTOM</b>	Message Transmission Optimization Mechanism
<b>N</b>	
<b>NAT</b>	network address translation
<b>ND</b>	Network Deployment
<b>NFS</b>	Network File System
<b>NG</b>	New Generation
<b>NIC</b>	network interface card
<b>NSS</b>	Network Security Services
<b>NSTISSC</b>	National Security Telecommunications and Information Systems Security Committee
<b>NTP</b>	Network Time Protocol
<b>O</b>	
<b>OASIS</b>	Organization for the Advancement of Structured Information Standards
<b>ODC</b>	on demand configuration
<b>ODR</b>	on demand router
<b>OID</b>	object ID
<b>OSI</b>	Open Systems Interconnection
<b>OTMA</b>	Open Transaction Management Access
<b>OVA</b>	open virtual appliance
<b>P</b>	
<b>PAM</b>	Pluggable Authentication Module
<b>PC</b>	Personal computer
<b>PCF</b>	Processing Control File
<b>PCRE</b>	Perl-compatible regular expressions
<b>PDF</b>	Portable Document Format
<b>PDP</b>	policy decision point
<b>PED</b>	PIN Entry Device
<b>PEP</b>	policy enforcement point
<b>PI</b>	processing instruction
<b>PIN</b>	personal identification number
<b>PKCS</b>	Public Key Cryptography Standard

<b>PKI</b>	public key infrastructure
<b>PKIX</b>	Public Key Infrastructure for X.509 Certificates (IETF)
<b>PMR</b>	program maintenance request

**Q**

<b>QA</b>	quality assurance
<b>QoS</b>	Quality of service

**R**

<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RAID</b>	Redundant Array of Independent Disks
<b>RAM</b>	random access memory
<b>RBM</b>	role-based management
<b>RDBMS</b>	relational database management system
<b>RDN</b>	relative distinguished name
<b>REL</b>	Rights Expression Language
<b>RFC</b>	Request for Comments
<b>RHEL</b>	Red Hat Enterprise Linux
<b>RSA</b>	Rational Software Architect

**S**

<b>SAF</b>	system authorization facility
<b>SAML</b>	Security Assertion Markup Language
<b>SAS</b>	Serial Attached SCSI
<b>SAX</b>	Simple API for XML
<b>SCP</b>	Secure Copy Protocol
<b>SCSI</b>	Small Computer System Interface
<b>SFP</b>	small-form-factor pluggable
<b>SFTP</b>	Secured File Transfer Protocol
<b>SHA1</b>	Secure Hash Algorithm, Version 1
<b>SLA</b>	service level agreement
<b>SLAAC</b>	stateless address autoconfiguration
<b>SLES</b>	SUSE Linux Enterprise Server
<b>SLM</b>	service level management
<b>SLM</b>	service level monitoring

<b>SMS</b>	session management server
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SOA</b>	Service-oriented architecture
<b>SOAP</b>	Usage note: SOAP is not an acronym; it is a word in itself (formerly an acronym for Simple Object Access Protocol)
<b>SOL</b>	serial over LAN
<b>SOMA</b>	service-oriented modeling and architecture
<b>SOMA</b>	SOAP management
<b>SPNEGO</b>	Simple and Protected GSS-API Negotiation Mechanism
<b>SQL</b>	Structured Query Language
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>SSO</b>	single sign-on
<b>SUSE</b>	Software und System Entwicklung (German for Software and Systems Development)
<b>SwA</b>	SOAP with Attachments

**T**

<b>Tcl</b>	Tool Control Language (often pronounced as “tickle”)
<b>TCO</b>	total cost of ownership
<b>TCP</b>	Transmission Control Protocol
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TDES</b>	Triple Data Encryption Standard
<b>TFIM</b>	Tivoli Federated Identity Manager
<b>TIA</b>	Telecommunications Industry Association
<b>TIM</b>	Tivoli Identity Manager
<b>TLS</b>	Transport Layer Security
<b>TTL</b>	Time to Live

**U**

<b>UDDI</b>	Universal Description, Discovery and Integration
<b>UDP</b>	User Datagram Protocol
<b>UNIX</b>	Uniplexed Information and Computing System
<b>URI</b>	Uniform Resource Identifier

<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>UTC</b>	Coordinated Universal Time

**V**

<b>VE</b>	Virtual Enterprise
<b>VIP</b>	virtual IP address
<b>VM</b>	Virtual machine
<b>VLAN</b>	virtual local area network
<b>VRRP</b>	Virtual Router Redundancy Protocol

**W**

<b>W3C</b>	World Wide Web Consortium
<b>WAFW</b>	Web application firewall
<b>WLC</b>	weighted least connections
<b>WLM</b>	workload management
<b>WLOR</b>	weighted least outstanding requests
<b>WML</b>	Wireless Markup Language
<b>WS</b>	web services
<b>WSDL</b>	Web Services Description Language
<b>WSDM</b>	Web Services Distributed Management
<b>WWW</b>	World Wide Web

**X**

<b>XCF</b>	cross-system coupling facility
<b>XCFG</b>	XML configuration
<b>XDoS</b>	XML denial of service
<b>XHTML</b>	Extensible Hypertext Markup Language
<b>XMI</b>	XML Management Interface
<b>XML</b>	Extensible Markup Language
<b>XMLDS</b>	XML digital signature
<b>XML-PI</b>	XML processing instructions
<b>XPath</b>	XML Path Language
<b>XSD</b>	XML Schema Definition
<b>XSL</b>	Extensible Stylesheet Language

**XSLT** Extensible Stylesheet Language Transformation

**Y**

**Z**

**z/OS** zSeries operating system



IBM Training



© Copyright International Business Machines Corporation 2018.