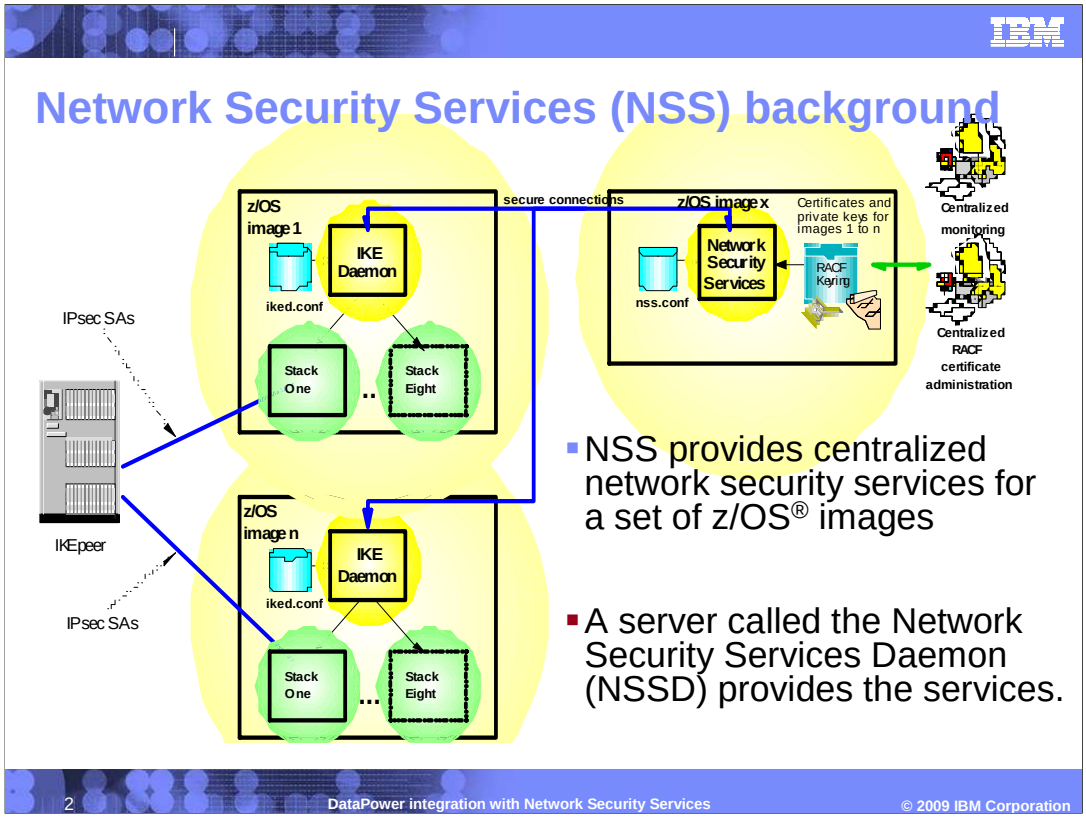
This presentation will discuss DataPower® integration with Network Security Services.



Network Security Services (NSS) performs the following functions:

It provides a central SAF-enabled repository for RSA certificates along with signature services within the most trusted zones.

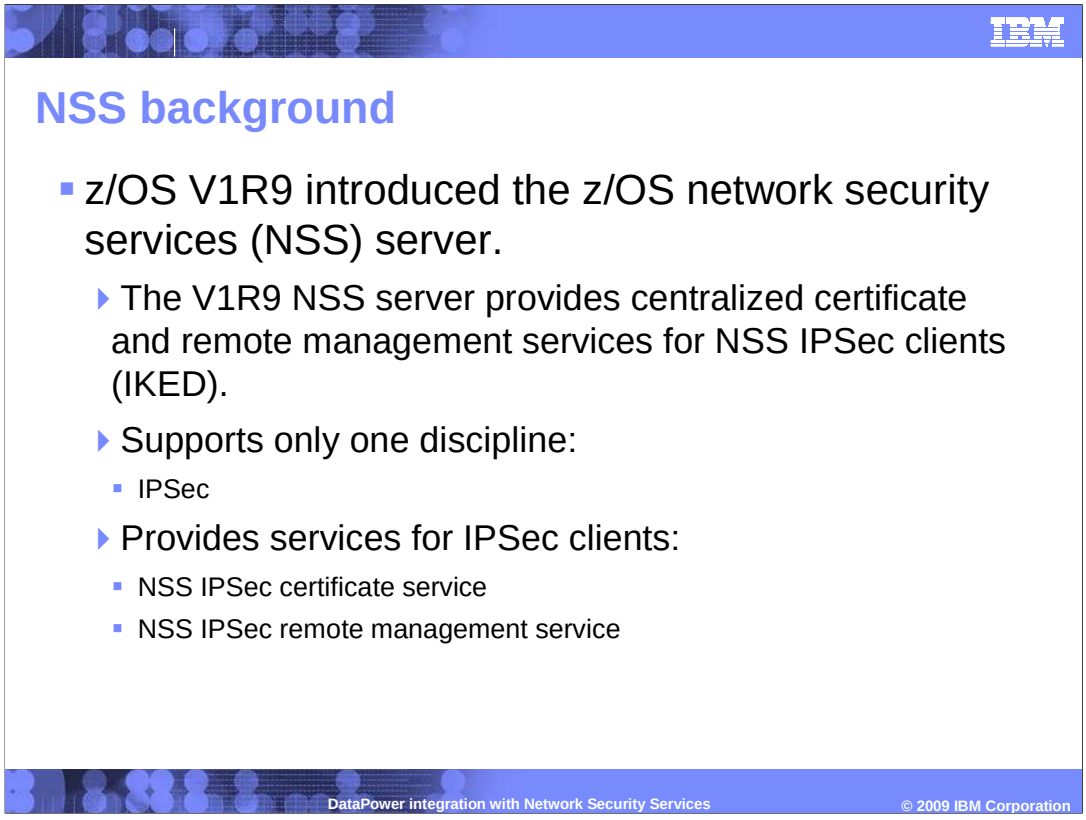
It eliminates the need to distribute certificates to security endpoints

It centralizes and reduces configuration and deployment complexity, especially when used along with Centralized Policy Services

It offloads digital signature operations from IKE daemon (the NSS client)

It enables monitoring and management of remote IPsec endpoints through the ipsec command and a network management programming interface.

The diagram on this page shows an NSS server on z/OS image X providing centralized certificate and private key services for IKE daemons running on z/OS Images 1 to n. Each z/OS Image has one Internet Key Exchange (IKE) daemon which serves all the stacks on that image. The IKE daemons act as clients to NSS, requesting certificate and private key services on behalf of the stacks they serve. An administrator using the ipsec command uses the NSS server on image X to monitor all the IKE daemons served by NSS. In this example, z/OS image X can also be in a more secure zone than the other images. This makes it safer to keep the keys and certificates there, rather than distributing them to the other z/OS images.



The network security services (NSS) server was added in z/OS V1R9 to support centralized certificate and remote management services for NSS IPSec clients. The IPSec certificate service provides digital signature creation and verification for remote NSS IPSec clients. This service permits multiple remote NSS IPSec clients, implemented by IKED, to store their authentication credentials in the form of x.509 certificates on a centralized z/OS server. This centralized approach to IPSec identity and certificate management eases the strain of certificate distribution throughout the enterprise.

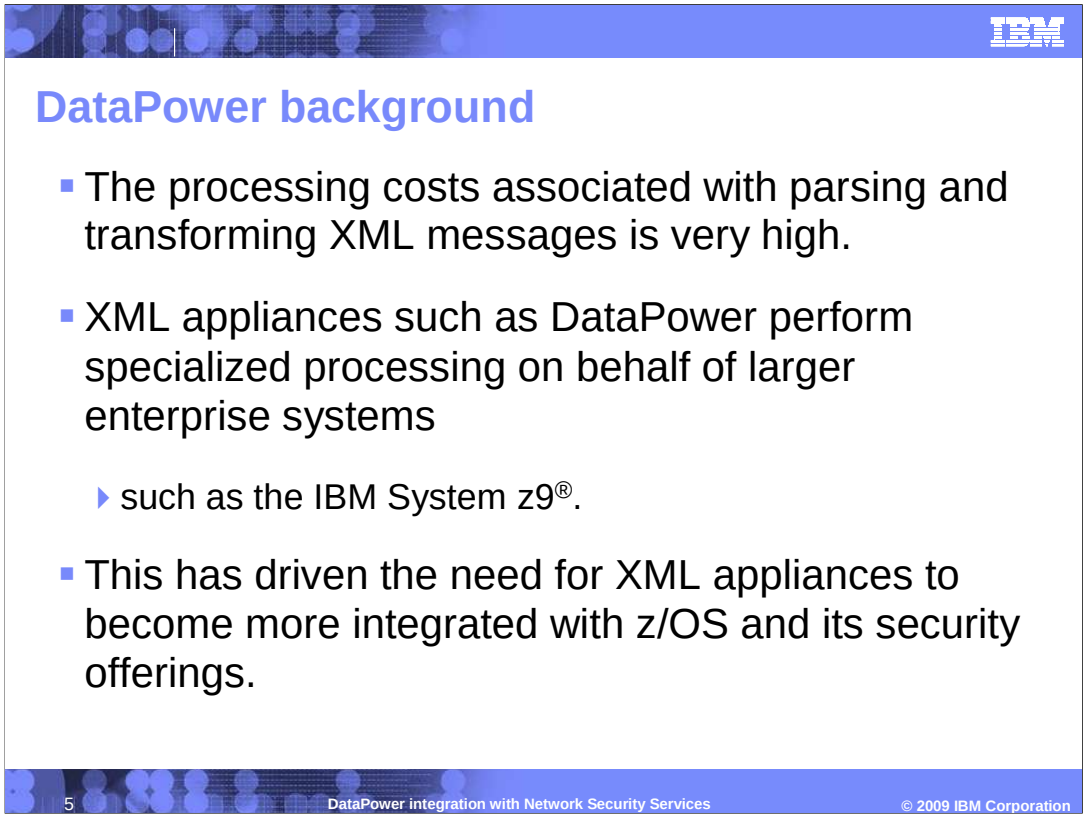
The IPSec remote management service complements the IPSec certificate service by allowing a locally run ipsec command to control and display security information for remote NSS IPSec clients (implemented by IKED).

NSS background

- The z/OS Internet Key Exchange Daemon (IKED) has NSS IPSec client functionality.
- The ipsec command uses NSS remote management service to monitor and control remote IPsec endpoints.

The z/OS V1R9 IKE daemon can be configured to act as an NSS IPSec client on behalf of multiple TCP/IP stacks. A separate connection is maintained to the NSS server for each NSS-enabled TCP/IP stack, so each TCP/IP stack is a separate NSS IPSec client to the NSS server. This allows a local ipsec administrator the ability to uniquely identify, administer, and observe the security of remote TCP/IP stacks acting as NSS IPSec clients.

The -z option of the ipsec command or other product use of the local NSS NMI can also be used to manage NSS IPSec clients authorized for the NSS remote management service.

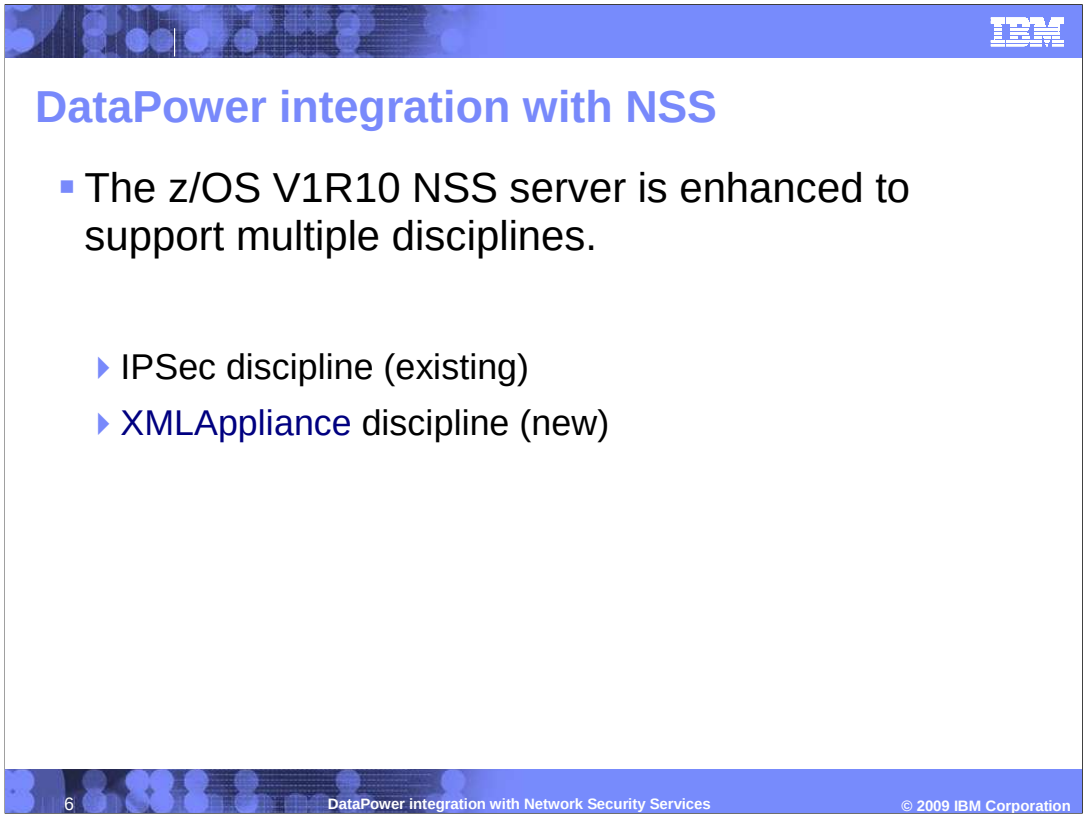


XML appliances secure and accelerate the parsing and transformation of many different types of messages, including XML-based messages. Examples of these appliances are the WebSphere® DataPower Integration Appliance XI50 and the WebSphere DataPower XML Security Gateway XS40.

The costs associated with parsing and transforming XML messages is extremely high. Since the volume and frequency of these messages are increasing, the deployment of specialized XML appliances has increased. Many of these appliances are now being used to simplify, secure, and accelerate the backend processing of these messages for larger enterprise systems such as IBM's System z9.

The increased deployment of XML appliances in this space requires tighter integration between the appliances and the z/OS security infrastructure.

The z/OS NSS server is well suited to provide the basic infrastructure for XML appliance security as it acts as a logical extension of z/OS security. The z/OS NSS server does this in z/OS V1R10 with new support for the XMLAppliance discipline.



The z/OS V1R10 NSS server is enhanced to add a new XMLAppliance discipline that provides the basic infrastructure for XML appliance security as it acts as a logical extension of z/OS security.

DataPower integration with NSS

- The NSS server can now provide services for both IPSec and XMLAppliance clients:
  - For IPSec clients:
    - NSS IPSec certificate service
    - NSS IPSec remote management service
  - For XMLAppliance clients (new):
    - NSS XMLAppliance SAF access service

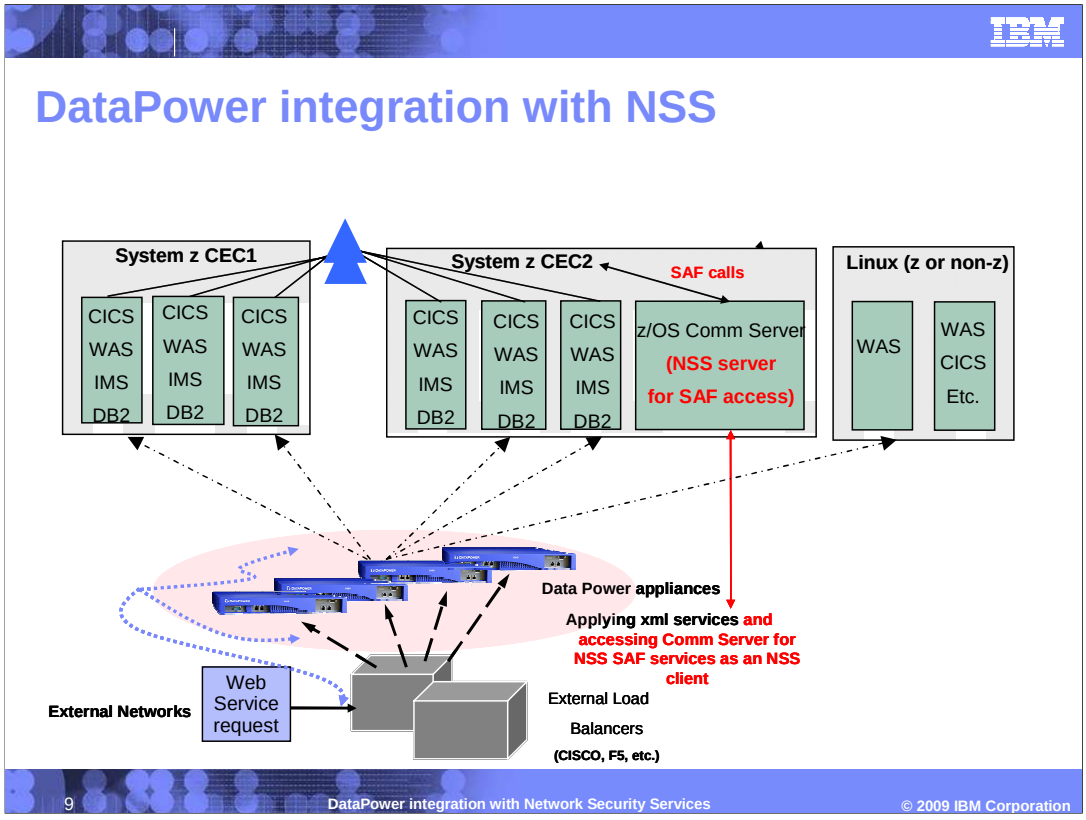
The new discipline adds one service to the NSS server: the XMLAppliance SAF access service provides the capability to invoke a selected set of SAF functions on behalf of its clients. Essentially, NSS becomes the conduit for making remote SAF calls.

An XML appliance connected to the NSS server can issue inline calls to the NSS server. These calls authenticate users and check whether users are authorized to perform certain actions on the appliance. The control of an XML appliance's users becomes centrally manageable and auditable from z/OS.

DataPower integration with NSS

- The new z/OS UNIX® nssctl command is implemented.
  - monitor the different types of NSS clients and their associated connections with NSS server.

A network administrator can monitor the different types of NSS clients and the associated client connections using the new z/OS UNIX nssctl command. Each type of NSS client will be in the client listing along with pertinent information. This information includes their NSS discipline, the services they are accessing, name, (connection) state, the time connected, the time of the last message received, the selected and enabled services, and other information.



Although the NSS SAF access service is an open interface and can be exploited by any XML Appliance, IBM Websphere Datapower SOA Appliances are currently the only known exploiter of the function.

This slide shows how the new NSS SAF access service might fit into a typical DataPower deployment.

The text and lines in red indicate new flows from DataPower appliances to the NSS server.

Network client traffic outside of the DataPower appliances and z/OS environment can be routed through a series of external load balancers before reaching the first DataPower appliance.

Each DataPower appliance can then be configured to act as one or more NSS XMLAppliance clients in order to use the new NSS SAF access service.

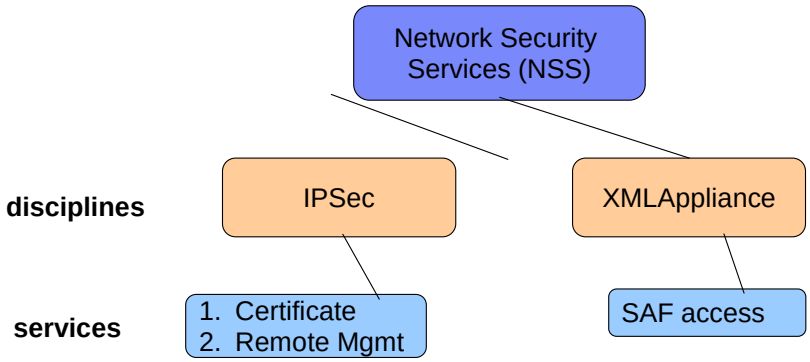
Traffic traveling through each DataPower appliance can cause it to issue a request to the NSS server in order to authenticate a client or to check the authorization of a client to a particular SAF resource. The NSS server then issues the request using the systems' SAF such as RACF® and responds directly to the DataPower appliance.

The rest of the DataPower appliance flow then proceeds as usual.

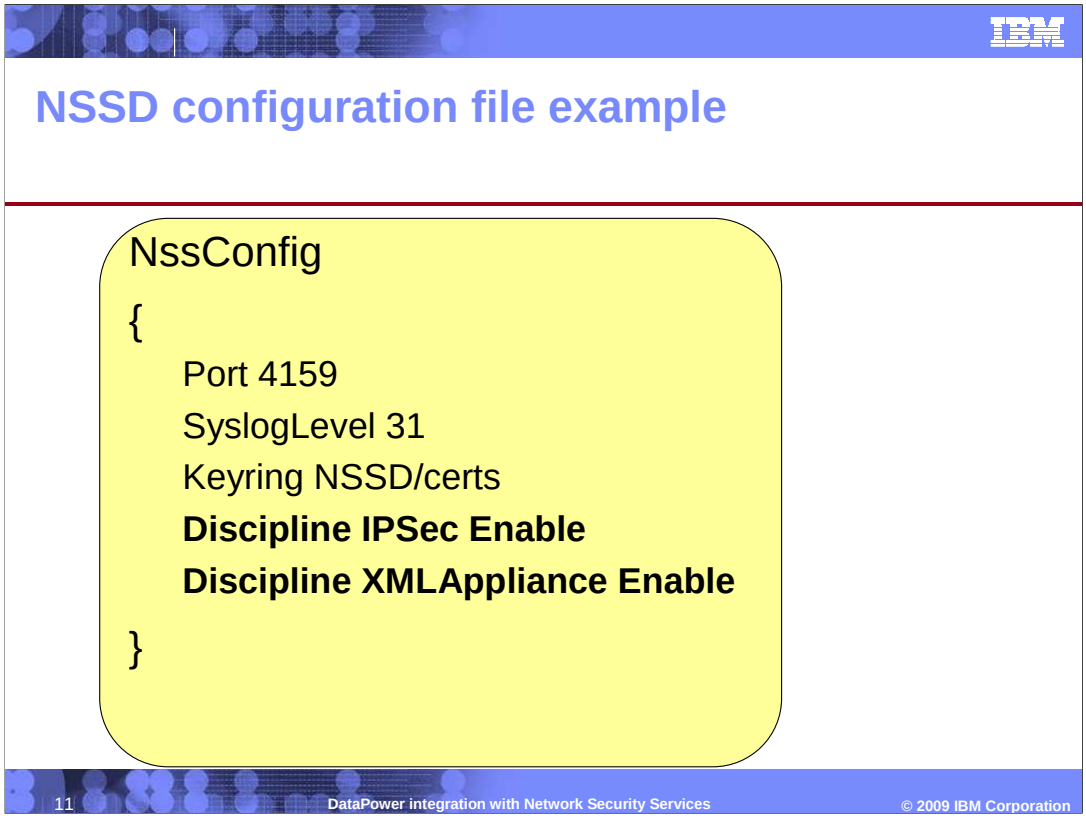
This type of configuration allows a z/OS security administrator to centrally manage authentication and authorization privileges for DataPower's clients. Such a configuration can easily replace LDAP as the central security solution for a DataPower appliance.

DataPower integration with NSS product level structure

NSS services by discipline:

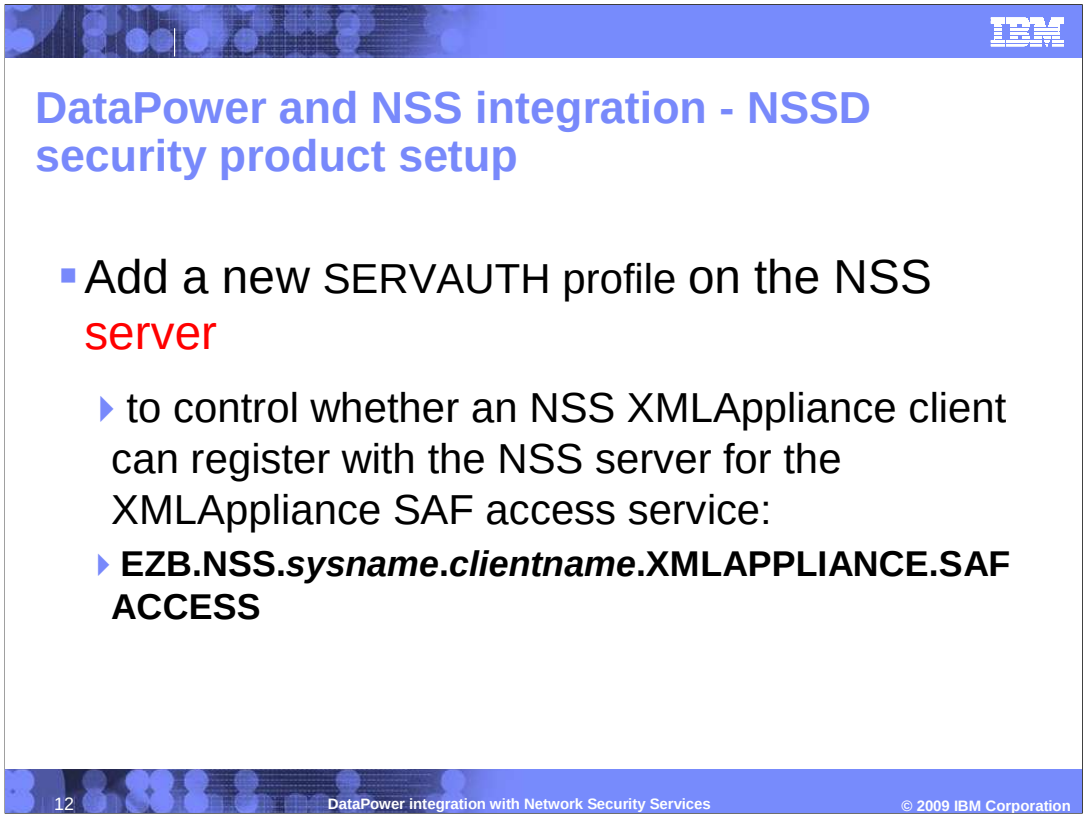


Network security services (NSS) provides discipline-specific security services for security integration, enforcement and management. Each discipline includes a set of services provided by NSS and is intended for use by a specific type of NSS client. This diagram illustrates that the new NSS server is becoming the hub for network security services and how those services are currently separated into their own disciplines. NSS clients can request and access services only relevant to the discipline specified at connect time. Certificate and remote management services are shown as only available under the IPSec discipline. SAF access is the only service available under the XMLAppliance discipline.



This is a sample configuration file for the z/OS V1R10 NSS server.

The port is specified as the default 4159 (IANA registered).
The syslog level is set to the max of 31.
The keyring is configured with owner NSSD and named 'certs'.
The IPSec discipline is set to enable.
The XMLAppliance discipline is set to enable.



This slide describes the NSSD security product setup.

(Note that the maximum allowable length of a SERVAUTH profile name is 64 characters)

The profile EZB.NSS.sysname.clientname.XMLAPPLIANCE.SAFACCESS controls whether an NSS XMLAppliance client can register with the NSS server for the XMLAppliance SAF access service.

- In this profile, *sysname* is the name of the z/OS system on which NSSD is running and *clientname* is the symbolic name of the NSS XMLAppliance client

An updated RACF sample (EZARACF) containing RACF commands for the XMLAppliance setup is provided with z/OS V1R10.

DataPower and NSS integration - commands

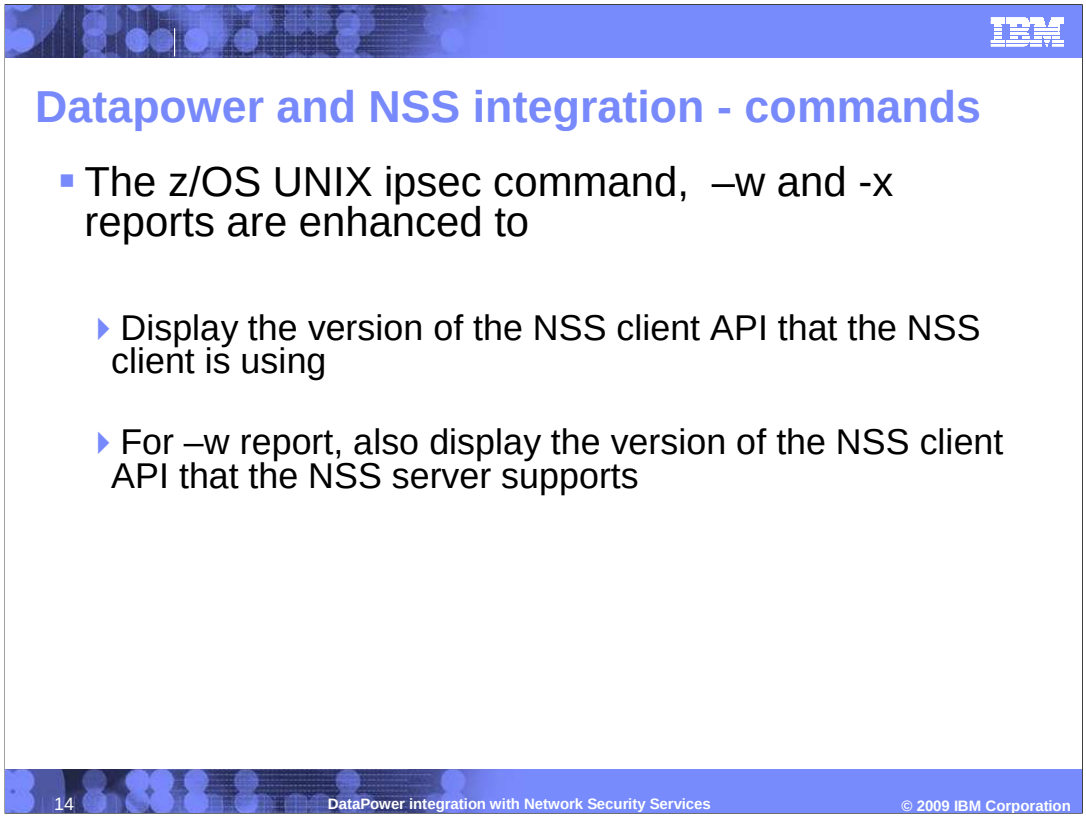
- New z/OS UNIX **nssctl** command:
  - Displays information for all NSS clients that are currently connected to the local NSS server.

Refer to the *IP System Administrator's Commands* book for detailed information about the new **nssctl** command syntax and parameter descriptions. You can also use command man page by issuing 'man nssctl'.

The **nssctl** command is an APF-authorized application. Users of the **nssctl** command must be authorized through the SERVAUTH profile EZB.NETMGMT.*sysname*.*sysname*.NSS.DISPLAY. *sysname* is the name of the z/OS system on which NSSD is running.

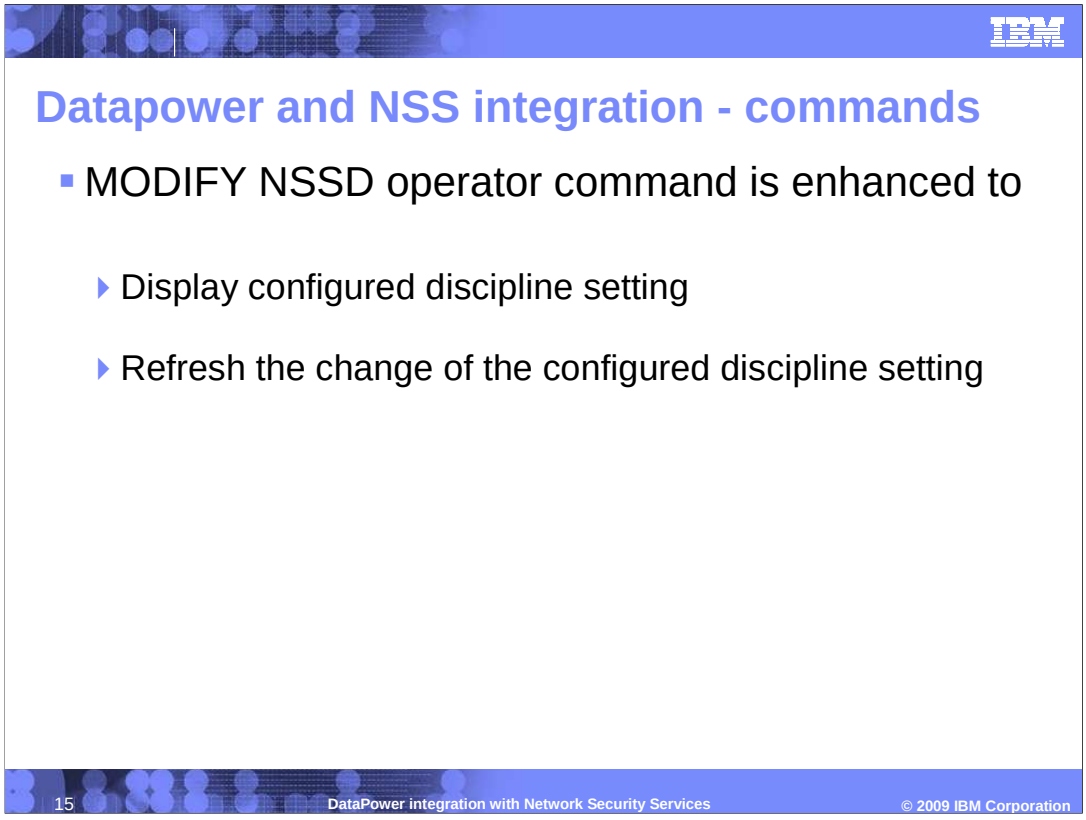
The most common usage of the nssctl command is "nssctl –d". This instructs the nssctl to 'display' ALL NSS clients. You can request only clients of a particular discipline by issuing "nssctl –d –D ipsec" to obtain information for all NSS IPSec clients. You can also filter on a client name by issuing "nssctl –d –c clientName1"

For command syntax help, you can issue "man nssctl" or "nssctl –?"



The **ipsec –w** option is directed at IKED and can be used to display network security configuration information for each active stack on the system.

The **ipsec –x** option is directed at NSSD and can be used to display information about NSS IPSec clients that are currently connected to the NSS server.



The MODIFY NSSD operator command is enhanced to display configured discipline setting and refresh the change of the configured discipline setting.

nssctl command report example - IPSec client

```
CS V1R10 nssctl  SystemName: MVS046    Tue Jan  8 18:05:10 2008
Function: Display            NSSClientName: n/a

ClientName:                      clientIB1
ClientAPIVersion:                2
StackName:                       tcpcs1
SystemName:                      zsystem2
ClientIPAddress:                 9.42.105.88
ClientPort:                      8801
ServerIPAddress:                 9.42.105.234
ServerPort:                      4159
UserID:                          userxyz
ConnectState:                    connected
TimeConnected:                   2008/01/08 18:05:08
TimeOfLastMessageFromClient:     2008/01/08 18:05:08
Discipline:                      IPSec
  CertificateServiceSelected:    Yes
  CertificateServiceEnabled:     Yes
  RemoteManagementSelected:      Yes
  RemoteManagementEnabled:       Yes
*************************************************************
```

Continued in the next page →

The nssctl command report includes information similar to that of the ipsec –x disp command.

NSS client information, such as ClientName, ClientAPIVersion, ClientIPAddress, ClientPort, UserID, ConnectState, TimeConnected, and TimeOfLastMessageFromClient….. are all common between the ipsec –x display and nssctl –d command.

The nssctl command, in contrast to the ipsec command, provides information for all NSS Disciplines and the services selected and enabled for each discipline.

The two supported disciplines supported in z/OS V1R10, as mentioned earlier, are IPSec and XMLAppliance.

If an NSS client is registered as an IPSec client, as seen in the example on this slide, the two services available are the Certificate service and the Remote Management service. The fields below the Discipline line indicate whether the client selected a particular service (CertificateServiceSelected) and additionally whether the NSS client is authorized to that service (CertificateServiceEnabled).

Refer to the *IP System Administrator's Commands* book for more detailed information about the field descriptions.

nssctl command report example
XML applicance client

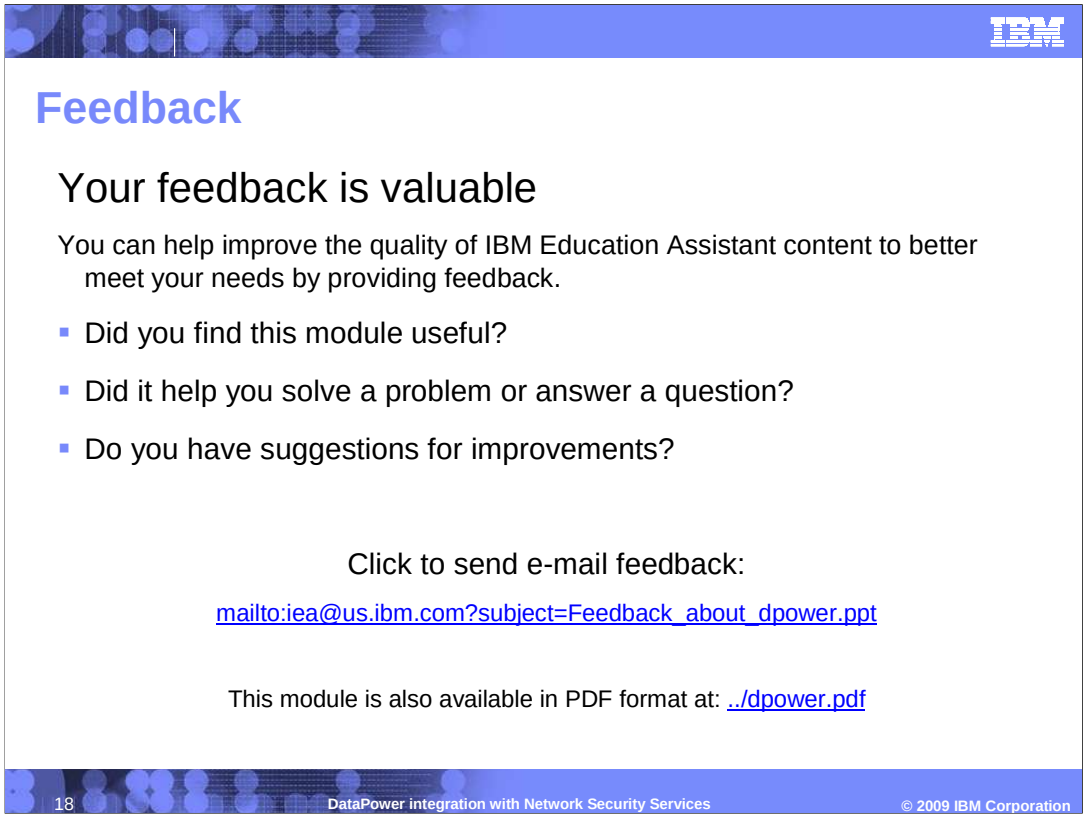
```
ClientName:                     ClientXB1
ClientAPIVersion:               2
StackName:                      Any
SystemName:                     dpsys01
ClientIPAddress:                ::ffff:10.11.1.5
ClientPort:                     1024
ServerIPAddress:                ::ffff:10.81.1.1
ServerPort:                     4159
UserID:                         USER5
ConnectState:                   connected
TimeConnected:                  2008/01/08 18:03:08
TimeOfLastMessageFromClient:    2008/01/08 18:05:02
Discipline:                     XMLAppliance
  SAFAccessServiceSelected:     Yes
  SAFAccessServiceEnabled:      Yes
************************************************************

2 entries selected
```


The NSS client seen in the example above is an XMLAppliance client.

In z/OS V1R10 the NSS XMLAppliance discipline supports one new service, the SAF access service.

For an NSS XMLAppliance client, the nssctl command output indicates whether the client selected the SAF access service (SAFAccessServiceSelected) and whether it is authorized to use this service (SAFAccessServiceEnabled).

Refer to the *IP System Administrator's Commands* book for more detailed information about the field descriptions.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

DataPower RACF System z System z9 WebSphere z/OS

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

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

Other company, product, or service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. 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 in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

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

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.