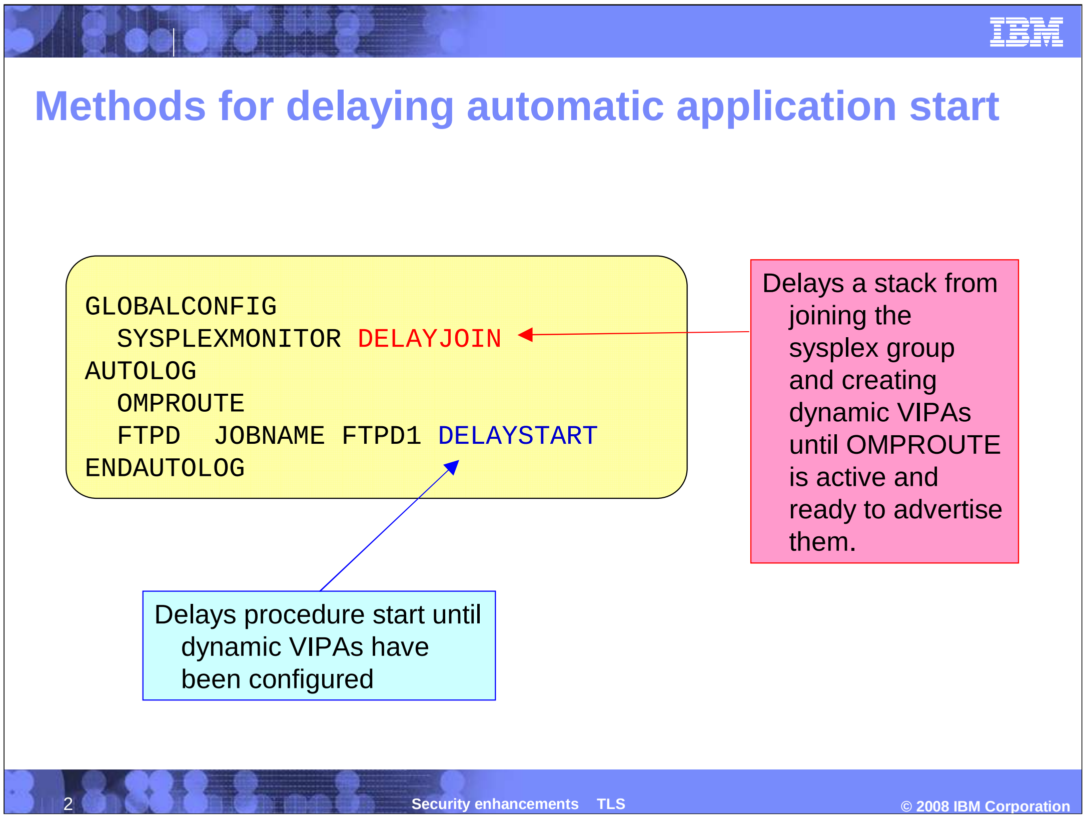
z/OS® V1R10 Communications Server

Security enhancements -- TLS

@business on demand software

This presentation covers enhancements made in the area of TLS security



Methods for delaying automatic application start

```
GLOBALCONFIG
  SYSPLEXMONITOR DELAYJOIN
AUTOLOG
  OMPROUTE
  FTPD  JOBNAME FTPD1 DELAYSTART
ENDAUTOLOG
```

Delays a stack from joining the sysplex group and creating dynamic VIPAs until OMPROUTE is active and ready to advertise them.

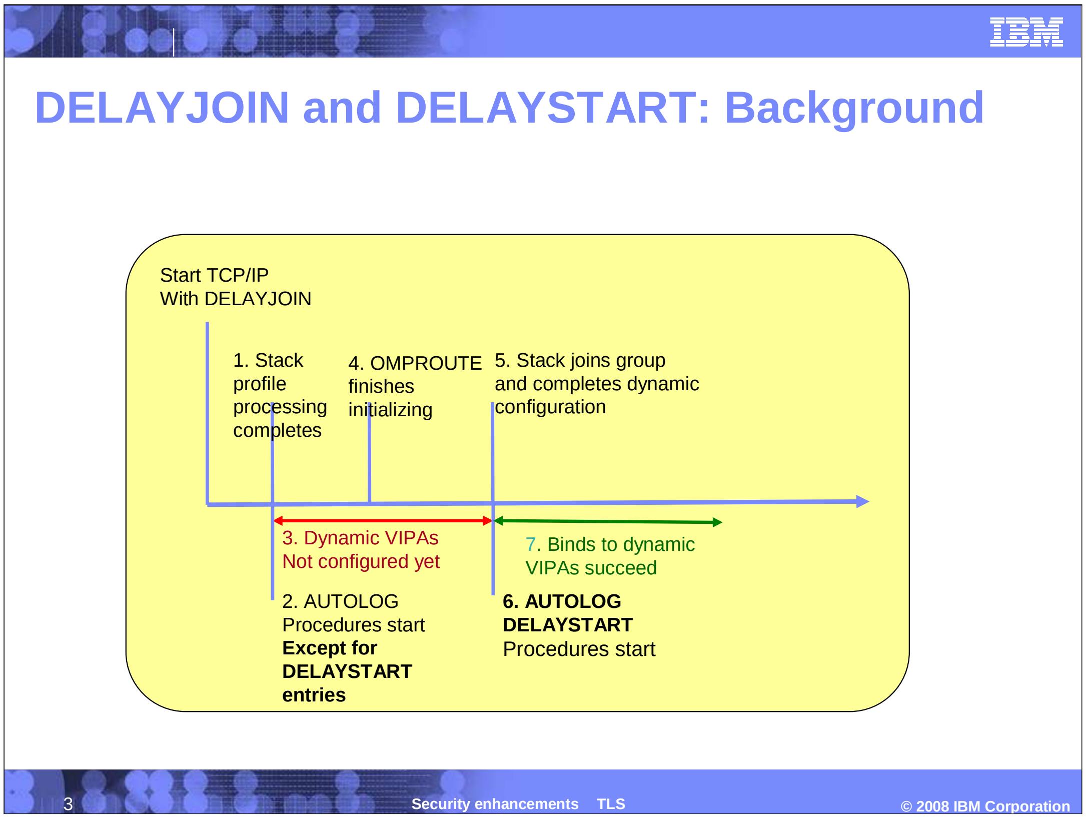
Delays procedure start until dynamic VIPAs have been configured

DELAYSTART is used so that AUTOLOG procedures that bind to a DVIPA will not start until the Dynamic VIPA (DVIPA) has been configured (after the stack has joined the sysplex group).

DELAYSTART is needed when DELAYJOIN is specified on the GLOBALCONFIG profile statement. When DELAYJOIN is specified, TCP/IP will not join the sysplex group and process the stack’s dynamic VIPA configuration until OMPROUTE is active and ready to advertise dynamic VIPAs. This prevents dynamic VIPAs from being created before they can be advertised by OMPROUTE.

What are some uses for DELAYJOIN? Consider this scenario.

Stack A joins the sysplex group and creates a dynamic VIPA which was previously active on Stack B. This causes Stack B to give up ownership of the DVIPA to Stack A; Stack B stops advertising the DVIPA. Stack B might have existing connections using the DVIPA. As part of the DVIPA takeback, Stack A also takes over routing packets for those connections to stack B so that the connections might continue. But, retransmits will occur on those connections until OMPROUTE is active and advertising the DVIPA on Stack A. By coding DELAYJOIN, Stack A will not create the DVIPA and take over ownership until OMPROUTE is ready to advertise the DVIPA



DELAYJOIN and DELAYSTART: Background

Start TCP/IP
With DELAYJOIN

1. Stack profile processing completes

2. AUTOLOG Procedures start **Except for DELAYSTART entries**

3. Dynamic VIPAs Not configured yet

4. OMPROUTE finishes initializing

5. Stack joins group and completes dynamic configuration

6. AUTOLOG DELAYSTART Procedures start

7. Binds to dynamic VIPAs succeed

The slide contains a time line showing the interaction of GLOBALCONFIG DELAYJOIN with the AUTOLOG DELAYSTART parameter

1.The stack completes initialization and finishes profile processing with the exception of the VIPADYNAMIC block.

2.AUTOLOG starts procedures that do not have DELAYSTART specified.

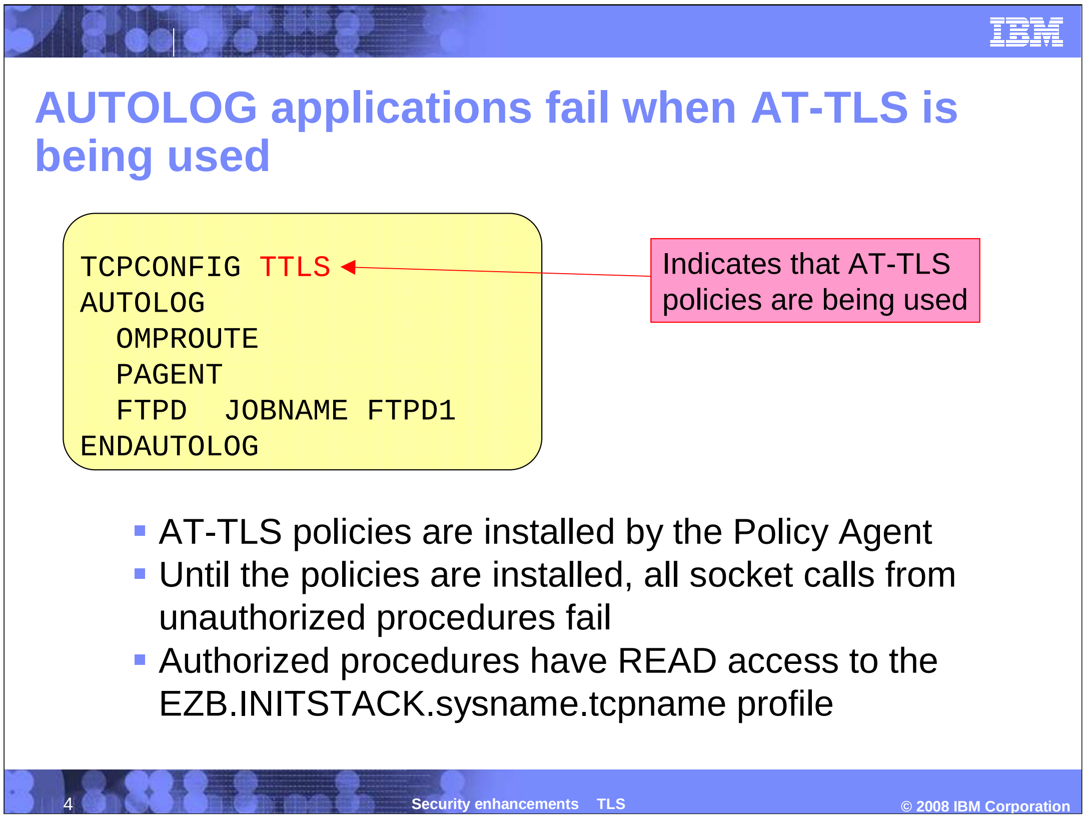
3.Dynamic VIPAs are not configured yet, so during this time period, a procedure attempting to Bind to a DVIPA will fail.

4.OMPROUTE completes initialization and notifies the stack.

5.The stack joins the sysplex group and processes its dynamic configuration creating dynamic VIPAs. The stack notifies AUTOLOG to start DELAYSTART procedures.

6.AUTOLOG starts the DELAYSTART procedures.

7.Binds from these procedures using DVIPAs are successful.



AUTOLOG applications fail when AT-TLS is being used

```
TCPCONFIG TTLS
AUTOLOG
  OMPROUTE
  PAGENT
  FTPD  JOBNAME FTPD1
ENDAUTOLOG
```

Indicates that AT-TLS policies are being used

- AT-TLS policies are installed by the Policy Agent
- Until the policies are installed, all socket calls from unauthorized procedures fail
- Authorized procedures have READ access to the EZB.INITSTACK.sysname.tcpname profile

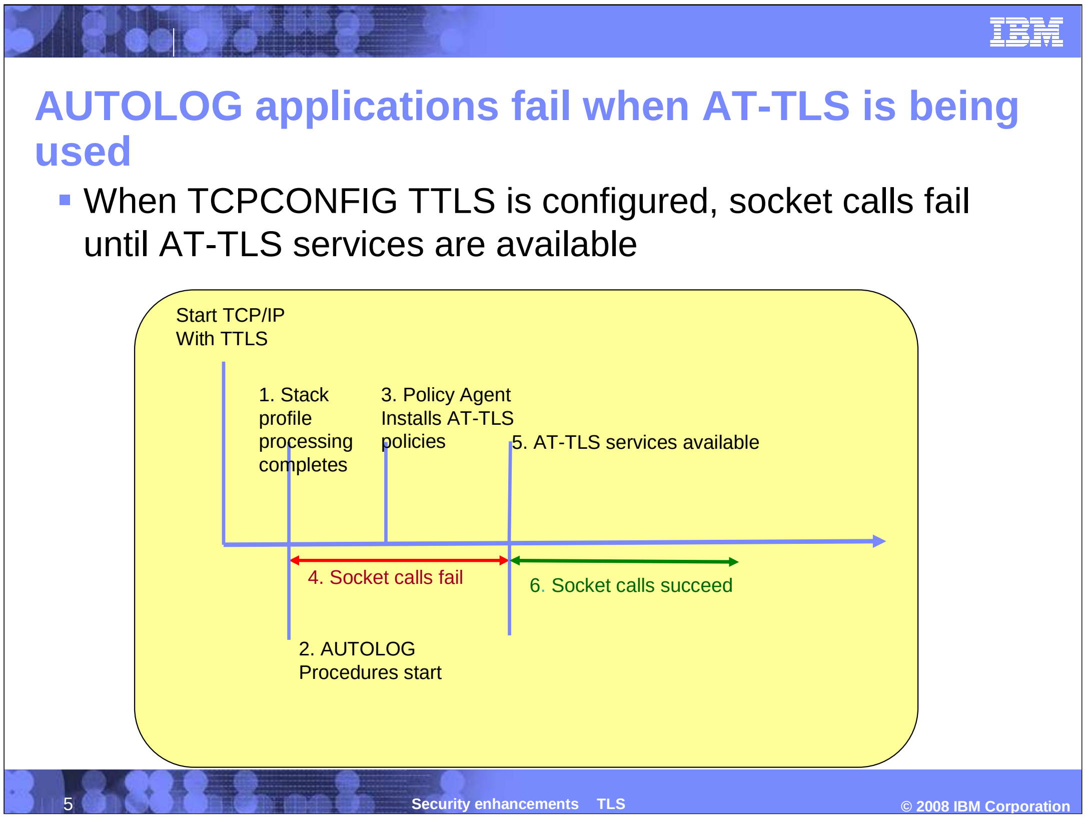
4 Security enhancements TLS © 2008 IBM Corporation

TCPCONFIG TTLS is configured in the TCP/IP profile to indicate that AT-TLS services are being used. AT-TLS requires AT-TLS policies to determine if a connection will use AT-TLS services and the type of AT-TLS services needed. Until the Policy Agent installs the AT-TLS policies, socket calls from unauthorized procedures fail.

Unauthorized procedures are those that do not have READ access to the RACF profile EZB.INITSTACK.*sysname*.*tcpname* in the SERVAUTH class.

A limited set of administrative applications such as Policy Agent and OMPROUTE need to be previously defined with access to this RACF resource. For example, this allows the Policy Agent to open a socket to the stack to install policies.

So in the example, OMPROUTE and PAGENT start successfully since they are authorized procedures, but the FTPD socket call fails if AT-TLS policies have not been installed. FTPD is not typically be authorized to the INITSTACK profile.



AUTOLOG applications fail when AT-TLS is being used

- When TCPCONFIG TTLS is configured, socket calls fail until AT-TLS services are available

Start TCP/IP With TTLS

1. Stack profile processing completes

3. Policy Agent Installs AT-TLS policies

5. AT-TLS services available

4. Socket calls fail

6. Socket calls succeed

2. AUTOLOG Procedures start

5 Security enhancements TLS © 2008 IBM Corporation

The diagram on this slide depicts this sequence of events:

1.The stack completes initialization and finishes profile processing.

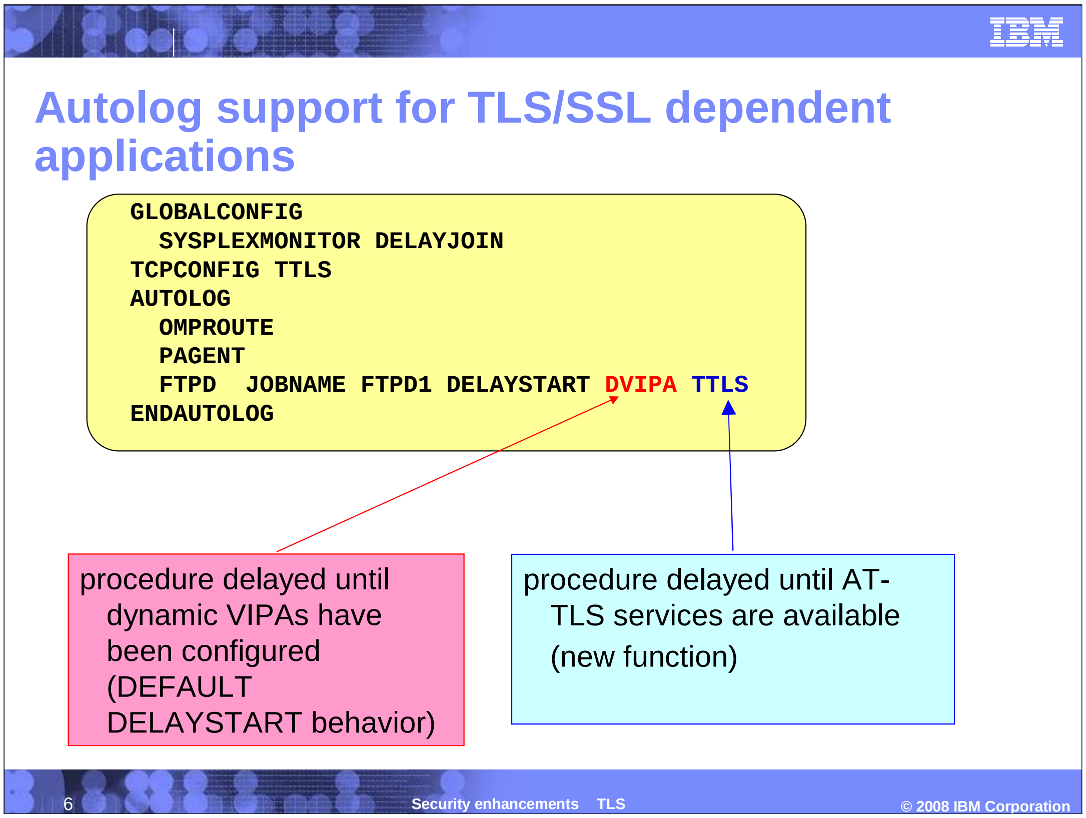
2.AUTOLOG procedures not configured with DELAYSTART are started

3.The Policy Agent installs AT-TLS policies.

4.Socket calls from unauthorized procedures fail during this time, because AT-TLS polices are not yet available. Autolog will restart the failing procedure after 5 minutes if the procedure has a reserved port in the profile

5.When all policies are installed, AT-TLS services are available.

6.Now that AT-TLS services are available, socket calls succeed.



Autolog support for TLS/SSL dependent applications

```
GLOBALCONFIG
  SYSPLEXMONITOR DELAYJOIN
TCPCONFIG TTLS
AUTOLOG
  OMPROUTE
  PAGENT
  FTPD  JOBNAME FTPD1 DELAYSTART DVIPA TTLS
ENDAUTOLOG
```

procedure delayed until dynamic VIPAs have been configured (DEFAULT DELAYSTART behavior)

procedure delayed until AT-TLS services are available (new function)

6 Security enhancements TLS © 2008 IBM Corporation

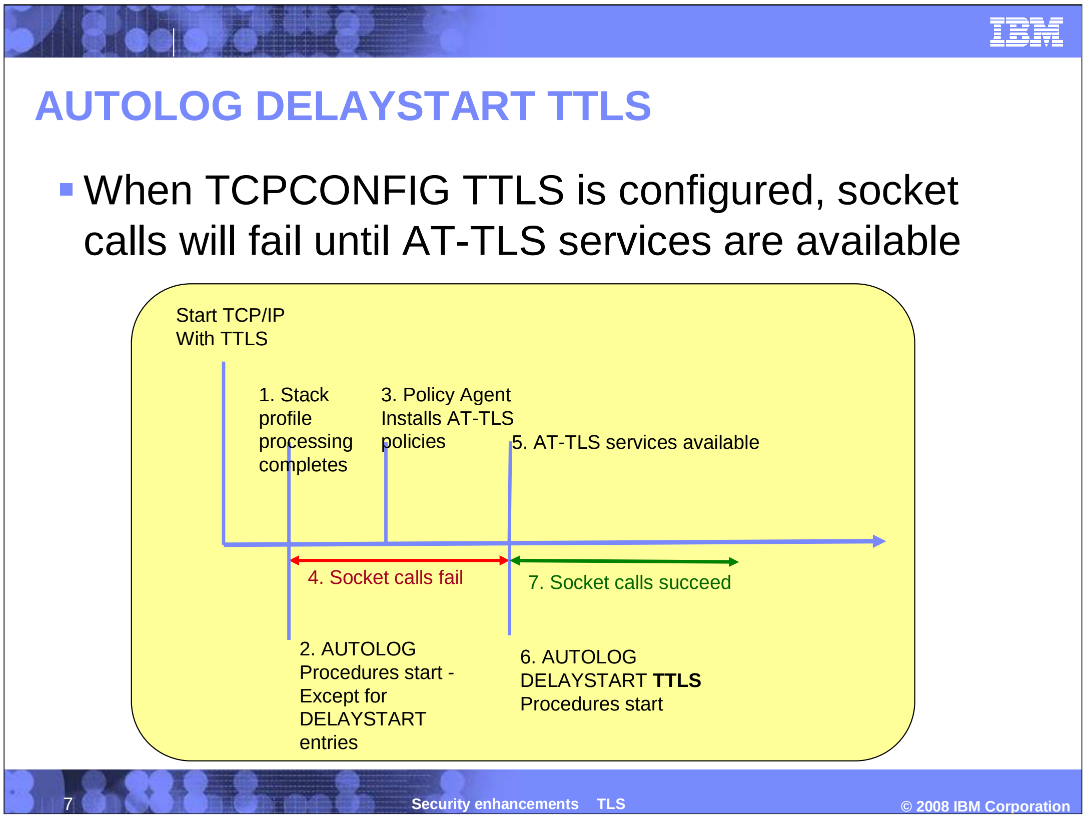
The problem described on the previous slides is solved in V1R10 by adding support for DELAYSTART parameters. The default is that DELAYSTART works as previously. Procedures are not started until dynamic VIPAs have been configured.

The new DVIPA parameter indicates that procedures are not to be started started until dynamic VIPAs have been configured. This is the same as the DEFAULT behavior.

The new TTLS parameter indicates that procedures are not to be started until AT-TLS policies have been installed and AT-TLS services are available.

When any parameter is present, there is no default behavior. To delay starting until dynamic VIPAs have been configured, DVIPA must be one of the parameters present.

In the example, both the DVIPA and TTLS parameters are present. In this case the procedure FTPD is not started until dynamic VIPAs have been configured and AT-TLS services are available.



AUTOLOG DELAYSTART TTLS

- When TCPCONFIG TTLS is configured, socket calls will fail until AT-TLS services are available

Start TCP/IP
With TTLS

1. Stack profile processing completes

3. Policy Agent Installs AT-TLS policies

5. AT-TLS services available

4. Socket calls fail

7. Socket calls succeed

2. AUTOLOG Procedures start - Except for DELAYSTART entries

6. AUTOLOG DELAYSTART **TTLS** Procedures start

This timeline shows the startup sequence when the new DELAYSTART TTLS parameter is configured on an AUTOLOG statement.

1.The stack completes initialization and finishes profile processing.

2.AUTOLOG procedures not configured with DELAYSTART are started

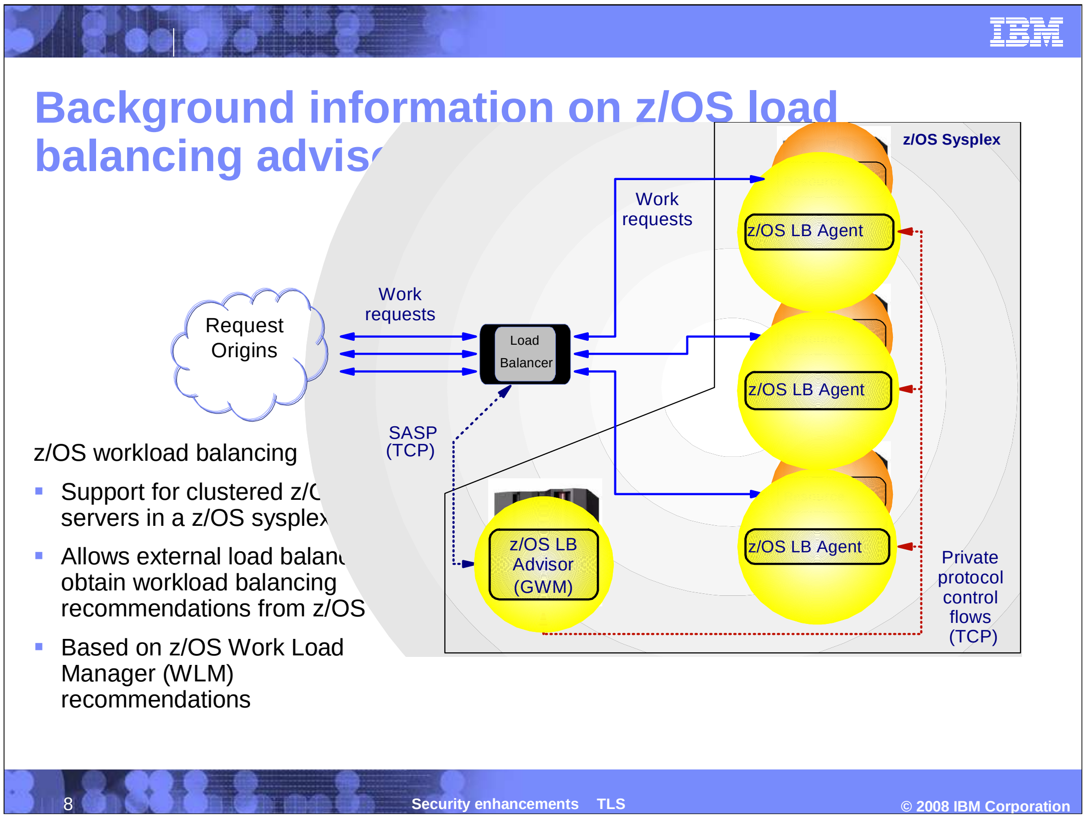
3.The Policy Agent installs AT-TLS policies.

4.Socket calls from unauthorized procedures fail during this time. Autolog will restart the failing procedure after 5 minutes if the procedure has a reserved port in the profile

5.When all policies are installed, AT-TLS services are available.

6.AUTOLOG DELAYSTART TTLS procedures are started

7.Socket calls succeed.



Background information on z/OS load balancing advis

z/OS workload balancing

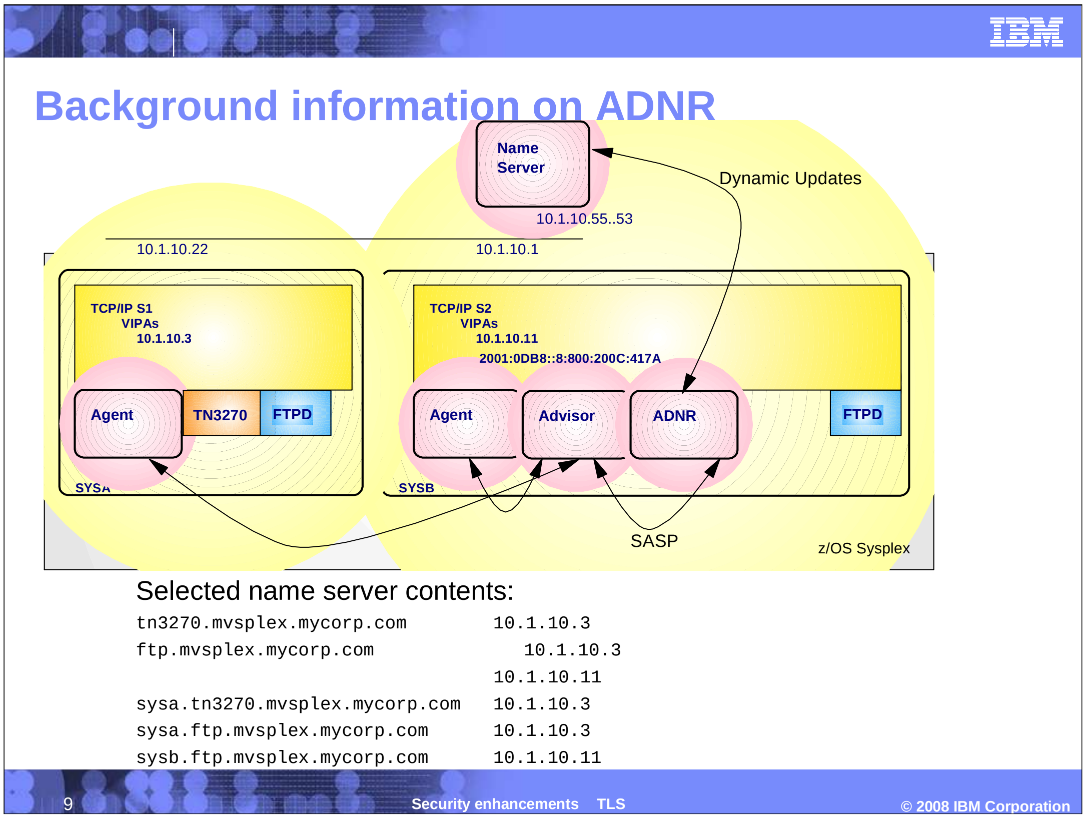
- Support for clustered z/C servers in a z/OS sysplex
- Allows external load balanc obtain workload balancing recommendations from z/OS
- Based on z/OS Work Load Manager (WLM) recommendations

The workload arrives from clients (leftmost in diagram). An external load balancer (center of the diagram) determines which server instance in the sysplex should receive a new workload using information from the z/OS Load Balancing Advisor. The Advisor collects load balancing data from Load Balancing Agents and sends recommendations to external load balancers. The load balancing data includes server availability, system capacity, and server ability to handle the new workload.

The z/OS Load Balancing Advisor solution consists of two z/OS applications. The Advisor is in the bottom-center of the diagram. There is one instance of the Advisor per sysplex. Or, if an MVS system spans multiple IP subplexes, each system has one instance of the Advisor for each IP subplex to which it belongs (as of V1R10). The Advisor communicates with external load balancers using the Server/Application State Protocol (SASP). The Advisor provides the role of a Global Workload Manager (GWM) in the SASP protocol. The Advisor provides external load balancers with information about z/OS resources. The Advisor collects information from Agents using a private protocol. The Advisor is a server application.

The Agents are the rightmost three z/OS images in the diagram. There is one instance of the Agent per MVS system. Or, if an MVS system spans multiple IP subplexes, each system has one instance of the Agent for each IP subplex to which it belongs (as of V1R10). The Agent collects information about z/OS systems and applications. The Agent sends information to the Advisor for aggregation using the private protocol. The Agent is a client application.

Note: The diagram does not show an Agent on the system where the Advisor is located, but this can be done and is required if applications on that system want to be targets of workload distribution.



Background information on ADNR

Selected name server contents:

```
tn3270.mvsplex.mycorp.com       10.1.10.3
ftp.mvsplex.mycorp.com             10.1.10.3
                                10.1.10.11
sysa.tn3270.mvsplex.mycorp.com  10.1.10.3
sysa.ftp.mvsplex.mycorp.com     10.1.10.3
sysb.ftp.mvsplex.mycorp.com     10.1.10.11
```

9 Security enhancements TLS © 2008 IBM Corporation

Automated domain name registration (ADNR) is an application that was introduced in V1R8. It provides automated DNS registration of application-specific host names. It is a client of the z/OS Load Balancing Advisor.

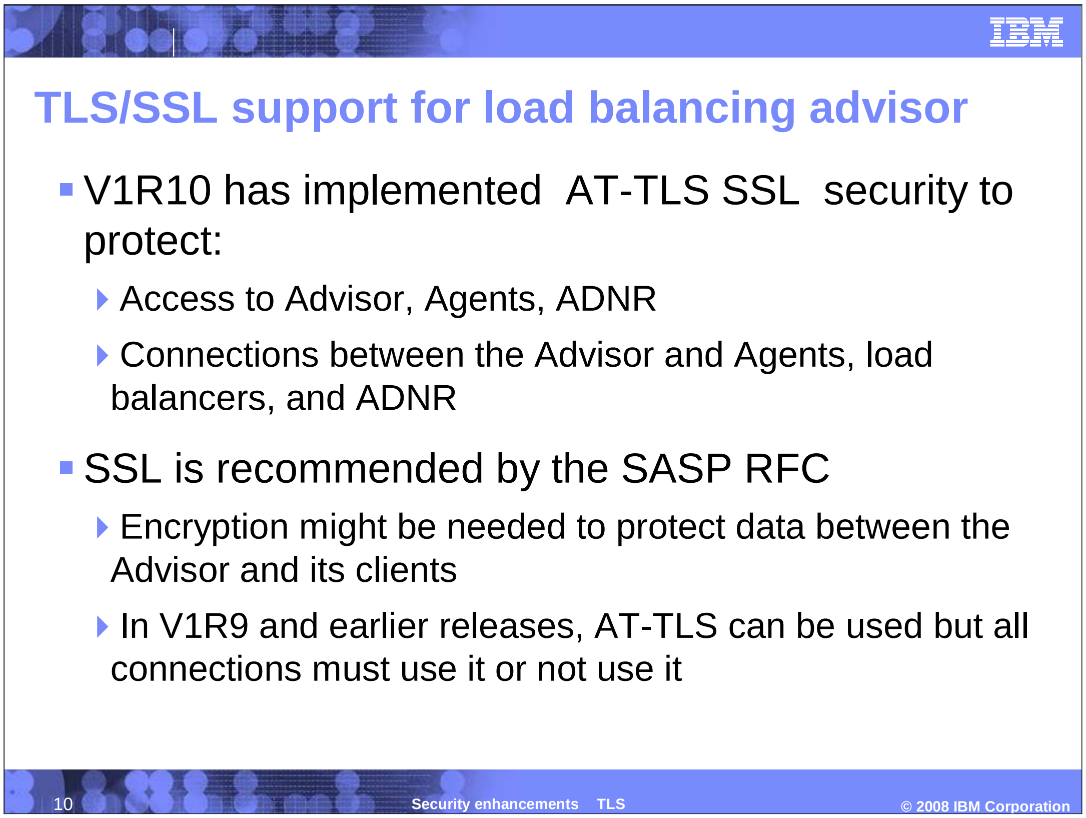
ADNR dynamically adds and deletes two types of host names in name servers. One type are application-specific host names and the addresses of those applications according to application availability. The other type are host names and their addresses representing a TCP/IP stack, MVS system, or subset of IP addresses.

ADNR provides a migration path for DNS/WLM users. DNS/WLM and BIND 4.9.3 support are planned to be removed in a subsequent release.

ADNR uses the z/OS Load Balancing Advisor, which is required for ADNR. ADNR looks like a load balancer to the Advisor application. Load balancing with external load balancers can coexist with ADNR.

In the slide drawing, the sysplex consists of two systems: SYSA and SYSB. SYSA has an Agent and two servers: TN3270 and FTPD. SYSB has the Advisor, an Agent, ADNR, and FTPD. The Advisor and ADNR are used for both systems in the sysplex. ADNR is configured with information about which sysplex resources to add to name server. ADNR’s configuration in this example includes TN3270 and FTPD server applications and the domain suffix to use ("mvsplex.mycorp.com"). FTP and TN3270 are the applications running in the sysplex. Note that ADNR supports a single server instance like TN3270 and groups of equivalent servers like FTP. The name server in this example is external to the sysplex. The name server might also reside on z/OS.

ADNR begins processing by registering configured application information (IP addresses, ports, and protocols) to the Load Balancing Advisor (LBA) Advisor. Both Agents monitor for application availability. Both Agents communicate changes in availability information to the Advisor. The Advisor relays availability information to ADNR. Finally, ADNR dynamically updates the name server with addresses and names representing the available applications (the names and addresses below the diagram).



IBM

TLS/SSL support for load balancing advisor

- V1R10 has implemented AT-TLS SSL security to protect:
  - Access to Advisor, Agents, ADNR
  - Connections between the Advisor and Agents, load balancers, and ADNR
- SSL is recommended by the SASP RFC
  - Encryption might be needed to protect data between the Advisor and its clients
  - In V1R9 and earlier releases, AT-TLS can be used but all connections must use it or not use it

10 Security enhancements TLS © 2008 IBM Corporation

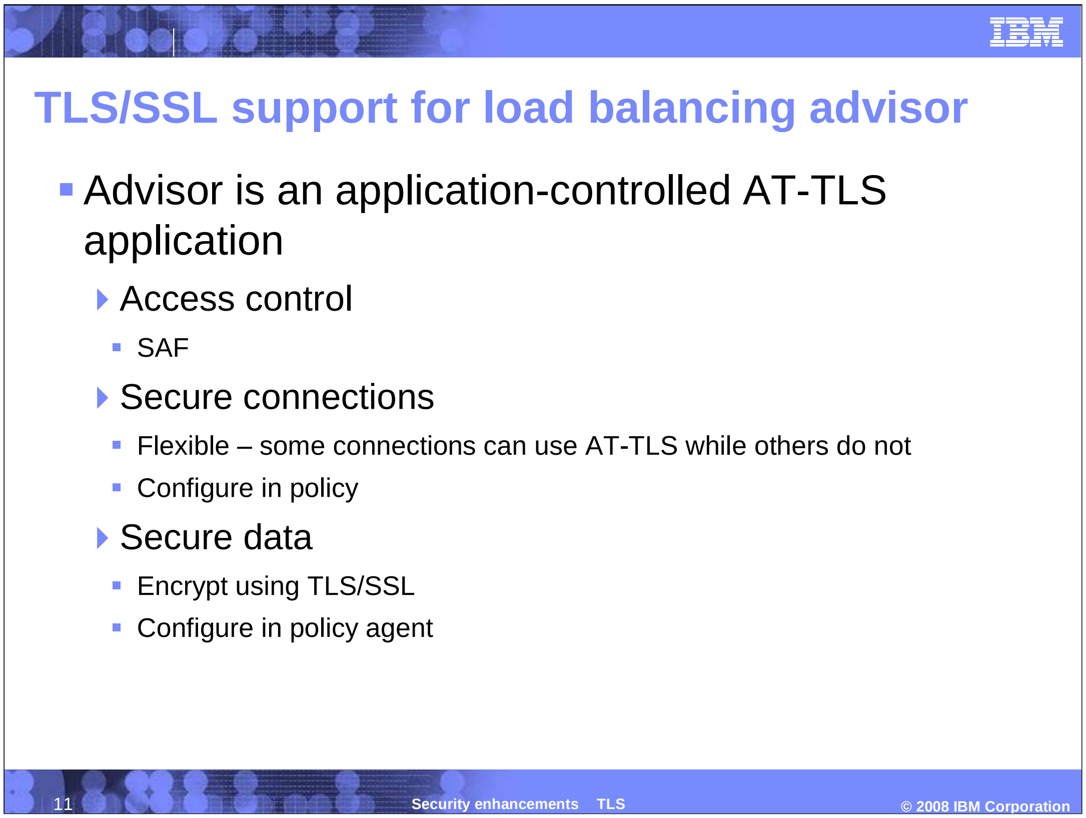
The Advisor, Agents, and ADNR are authorized programs which must be started from a start procedure. However, before V1R10, any user ID can establish a connection to the Advisor. The ability to establish a connection to the Advisor needs to be restricted to "authorized parties" as sensitive interfaces can be exploited once a connection is accepted by the LBA. You need to ensure that only Load Balancing Agents that IBM provides are allowed to connect to the Agent listening port. Agents are responsible for providing sensitive information that indicates server application availability, health and performance. You need to ensure that only authorized load balancers are allowed to connect to the Advisor on the external load balancer SASP port. The Advisor to load balancer interface can be used to obtain sensitive information regarding TCP/IP applications deployed in a sysplex, processor utilization information for each system, and so on.

In V1R9 and earlier releases, connections to the Advisor are controlled only by requiring the IP addresses of both ends of the connection to be configured on both applications. The configured IP addresses might be sufficient in certain user environments where the Load Balancing Advisor, Agents and external load balancers all reside inside a secure network (that is isolated by firewalls, and so on). However, they might not be viewed as sufficient in environments where the network is not considered to be as secure or where the need to protect against IP address spoofing attacks is important.

The SASP RFC 4678 Server/Application State Protocol v1 recommends SSL.

AT-TLS can be used before V1R10, but the Advisor in prior releases does not control connections from external load balancers, Agents, and ADNR, and the Advisor in prior releases does no access control. In addition, the Advisor in prior releases will not allow some clients to connect with AT-TLS and others to connect without AT-TLS.

The data flowing on the Advisor's connections, which includes server application availability, health, and performance, might need to be encrypted. An AT-TLS policy can specify encryption for data flowing outside of the TCP/IP stack. (Encryption is provided by AT-TLS and is not new in V1R10.)



IBM

TLS/SSL support for load balancing advisor

- Advisor is an application-controlled AT-TLS application
  - Access control
    - SAF
  - Secure connections
    - Flexible – some connections can use AT-TLS while others do not
    - Configure in policy
  - Secure data
    - Encrypt using TLS/SSL
    - Configure in policy agent

11 Security enhancements TLS © 2008 IBM Corporation

In z/OS V1R10 Communications Server, you can secure and control access to all communications with the Load Balancing Advisor using TLS/SSL technologies. The TLS/SSL support for the Load Balancing Advisor, Agents and the ADNR function is provided using the AT-TLS feature of the Communications Server.

With the LBA enhancements in V1R10, you have the ability to perform access control checks using SAF-compliant security product profiles.

In V1R10, you can authenticate external load balancers, z/OS Load Balancing Agents and ADNR clients connecting to the Load Balancing Advisor using client certificates.

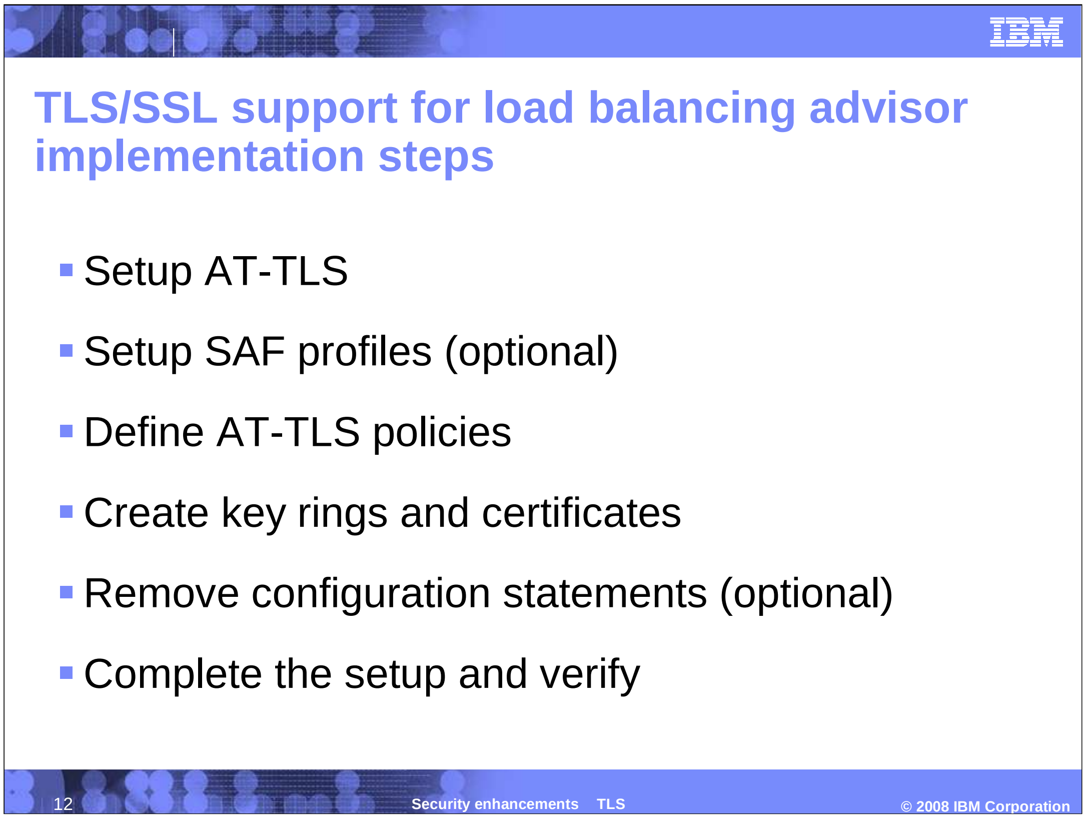
In V1R10, you can use a combination of TLS/SSL and non-TLS/SSL connections to the Advisor.

In V1R10, you can improve availability of the Advisor and Agents by removing some configuration statements. Before V1R10, adding an Agent or load balancer instance into the sysplex required updates to the Advisor configuration, which in turn requires a recycle of the Advisor as dynamic reconfiguration is not supported.

In V1R10, using AT-TLS, you can add an Agent or load balancer instance without impacting the Advisor.

In V1R10, you can encrypt data flowing between the Advisor’s TCP/IP stack and its clients (this support is provided by AT-TLS and is not new in V1R10).

SAF is the System Authorization Facility. Examples in this presentation use RACF.



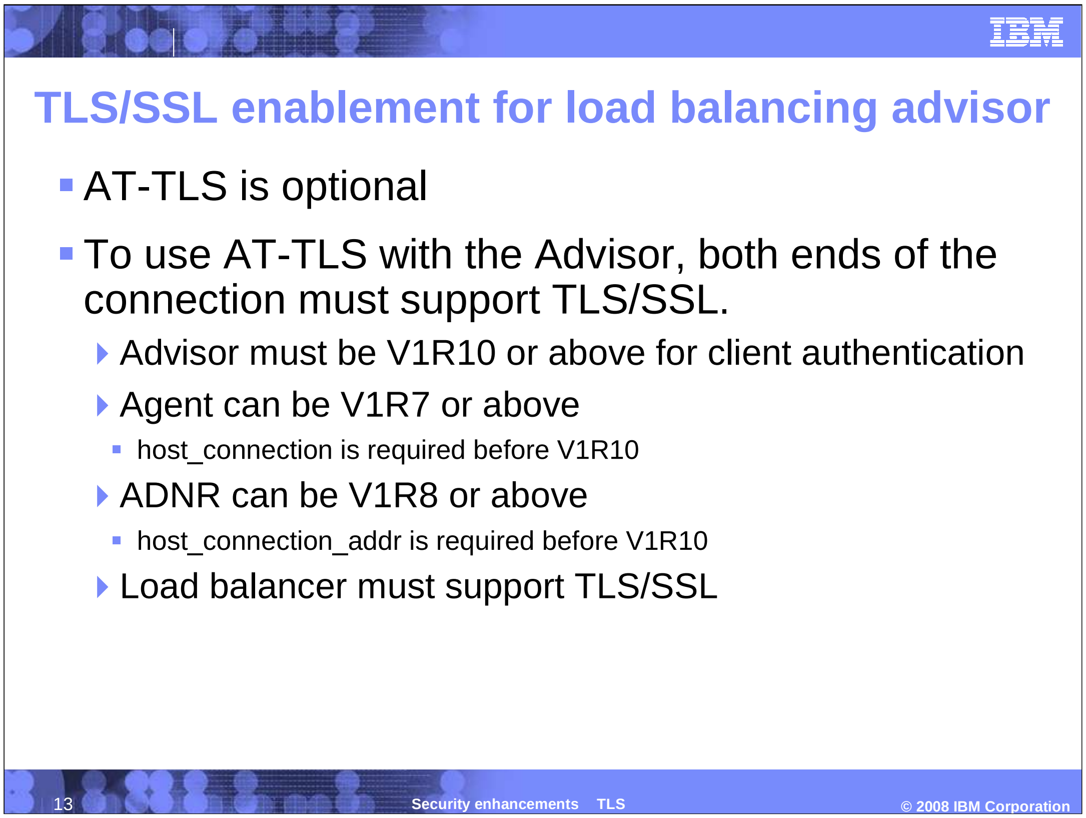
TLS/SSL support for load balancing advisor implementation steps

- Setup AT-TLS
- Setup SAF profiles (optional)
- Define AT-TLS policies
- Create key rings and certificates
- Remove configuration statements (optional)
- Complete the setup and verify

12 Security enhancements TLS © 2008 IBM Corporation

This slide is an overview of the steps to setup AT-TLS for the z/OS Load Balancing Advisor.

Assuming you are using the Policy Agent, additional steps are required to setup AT-TLS, if you have not already done so. You might want to setup new SAF profiles. You need to define new AT-TLS policies for the Policy Agent. You need to create key rings and certificates. You might want to remove the configuration statements that specify the IP addresses for the connections to the Advisor. Finally, you need to complete the setup and verify that the setup is correct.



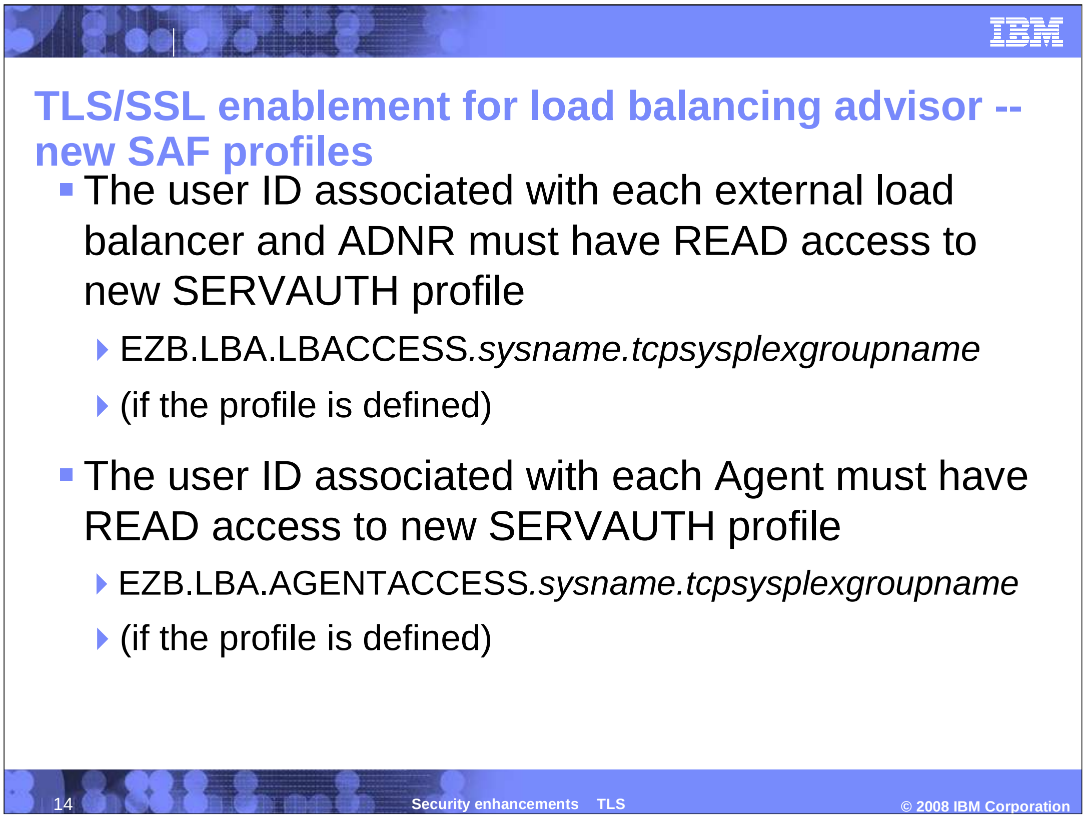
TLS/SSL enablement for load balancing advisor

- AT-TLS is optional
- To use AT-TLS with the Advisor, both ends of the connection must support TLS/SSL.
  - Advisor must be V1R10 or above for client authentication
  - Agent can be V1R7 or above
    - host_connection is required before V1R10
  - ADNR can be V1R8 or above
    - host_connection_addr is required before V1R10
  - Load balancer must support TLS/SSL

AT-TLS is optional. The Advisor, Agents and ADNR will continue to support the IP addresses in their configuration files. If AT-TLS is successfully used for a connection, the Advisor's configuration file statements for agent_id_list and lb_id_list is ignored for this connection. If AT-TLS is unsuccessful, message EZD1280I (described on a previous slide) is issued and in most cases the configuration file is used for authorization. The one exception is if the SAF profile (described on a previous slide) is defined but the user ID associated with the application does not have READ access to the SAF profile. In this case, the Advisor will reject the connection without checking the configuration file.

All connections are independent. You can use AT-TLS for some Agent connections and not for others, and at the same time, use AT-TLS for some load balancer connections and not for others. Any combination of AT-TLS and non-AT-TLS works.

To use AT-TLS with client authentication, access control, and encryption, both ends of the connection must support TLS/SSL. This means that the Advisor must be V1R10 or above for client authentication. The Agent can be any release above (and including) V1R7 (the release in which AT-TLS was added), but only V1R10 or above will allow the host_connection statement to be optional in the Agent configuration file. ADNR (which was introduced in V1R8) can be in any release, but only V1R10 or above will allow the host_connection_addr parameter to be optional in the ADNR configuration file. The external load balancer must support TLS/SSL.



TLS/SSL enablement for load balancing advisor -- new SAF profiles

- The user ID associated with each external load balancer and ADNR must have READ access to new SERVAUTH profile
  - EZB.LBA.LBACCESS.*sysname.tcpsysplexgroupname*
  - (if the profile is defined)
- The user ID associated with each Agent must have READ access to new SERVAUTH profile
  - EZB.LBA.AGENTACCESS.*sysname.tcpsysplexgroupname*
  - (if the profile is defined)

14 Security enhancements TLS © 2008 IBM Corporation

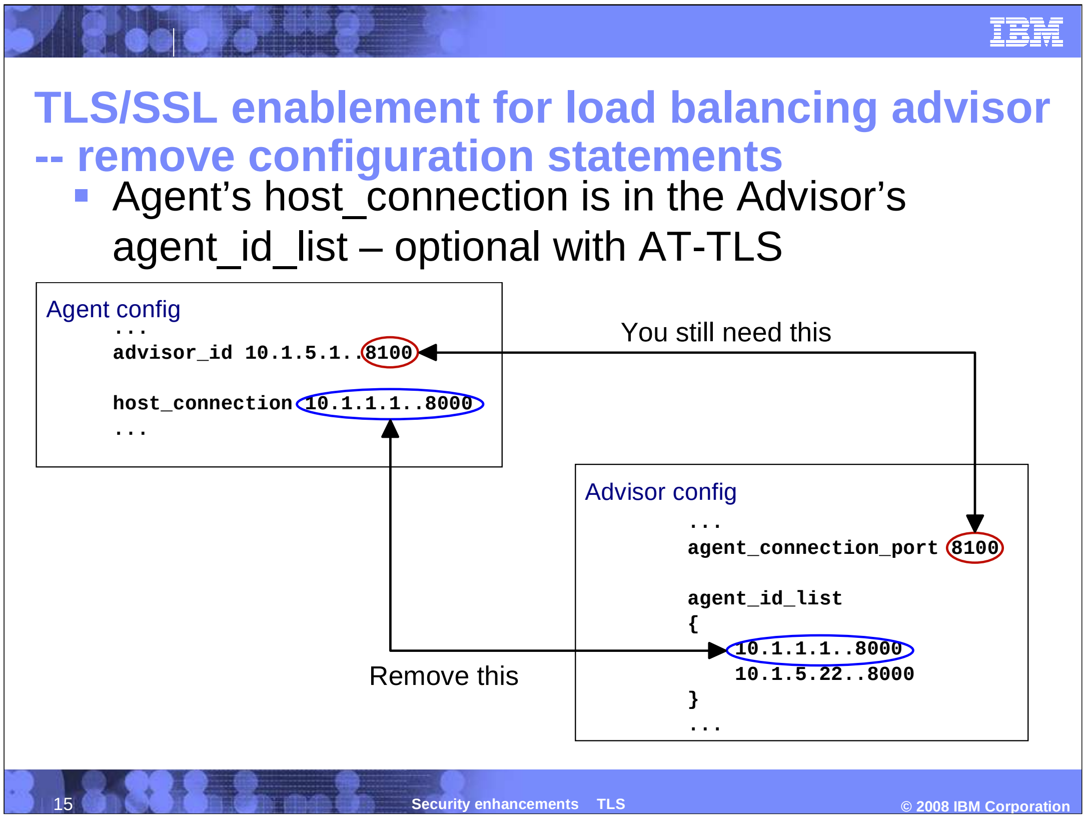
With an AT-TLS policy in place, the Load Balancing Advisor will only allow TCP connections that have met this criteria, in other words, connections that have been authenticated using TLS/SSL. Note however that there is still the issue of access control. That is, should a specific user be able to access the LBA resources associated with the port? The solution is to use a SAF resource (that is, RACF or equivalent ESM) profile to which the client's user ID must be explicitly permitted. If access control by way of SAF is desirable, define the necessary SERVAUTH profiles and permit authorized users to these profiles. If the appropriate SAF profile is defined, then only authorized Agents, external load balancers, and ADNR are allowed to connect to the Advisor.

The format of the SERVAUTH profile to authorize load balancer and ADNR connections is EZB.LBA.LBACCESS.*sysname.tcpsysplexgroupname* . The format of the SERVAUTH profile to authorize Agent connections is EZB.LBA.AGENTACCESS.*sysname.tcpsysplexgroupname*. Refer to the sample file, EZARACF.SAMPLE, for the specific RACF commands.

Each client must be permitted to the SERVAUTH profile if the profile is defined. ADNR and external load balancers must have at least READ access to the LBACCESS SERVAUTH profile. Agents must have at least READ access to the AGENTACCESS SERVAUTH profile. For an external load balancer, you create a user ID in the SAF product on z/OS which represents the external load balancer. This is the user ID that you give access to. For jobs running on z/OS, the user ID that must have the access can be found in message IEF695I in the system log and job log. In this example, the user ID is USER1 :

```
IEF695I START LBADV    WITH JOBNAME LBADV    IS ASSIGNED TO USER USER1   ,
GROUP SYS1
```

If the Advisor can run on more than one system, you need to setup the SAF controls on all of those systems. For more information about RACF, see *z/OS Security Server RACF Security Administrator's Guide.*



TLS/SSL enablement for load balancing advisor -- remove configuration statements

- Agent's host_connection is in the Advisor's agent_id_list – optional with AT-TLS

Agent config

```
     ...
     advisor_id 10.1.5.1..8100

     host_connection 10.1.1.1..8000
     ...
```

You still need this

Advisor config

```
         ...
         agent_connection_port 8100

         agent_id_list
         {
             10.1.1.1..8000
             10.1.5.22..8000
         }
         ...
```

Remove this

15 Security enhancements TLS © 2008 IBM Corporation

When not using AT-TLS for an Agent's connection to the Advisor, the IP address and port on the host_connection statement on the Agent must match an entry in the Advisor's agent_id_list statement. The slide also shows that the port on the Agent's advisor_id statement must be the same as the port on the Advisor's agent_connection_port statement.

The Agent's host_connection statement and the corresponding entry in the Advisor's agent_id_list are optional in V1R10 if AT-TLS is used for all connections between the Advisor and the Agent. (The advisor_id and agent_connection_port statements are still required when using AT-TLS.) Once you have AT-TLS connections working, you should remove these optional statements to ensure that non-secure connections are not allowed.

If you are using ADNR with the load balancing advisor, similar changes are needed. When configuring the Advisor and ADNR without AT-TLS, the host_connection_addr parameter on the ADNR gwm statement must match an entry in the Advisor's lb_id_list statement. These parameters are optional in V1R10 if AT-TLS is used for the connection between the Advisor and ADNR.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

z/OS

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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.

Information is provided "AS IS" without warranty of any kind. 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.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.