Agenda

Overview
- What is security?
- CIA Triangle
- QlikView in the CIA triangle
- Communication with IT

Components in QlikView 9
- Products
- Where do the products fit in?
- QlikView architecture back-end and front-end
- Security bullets regarding this design

Back-end security

Front-end security

Qonnections

Global Partner Summit 2010

MIAMI

What is information security?
Information Security according to Wikipedia

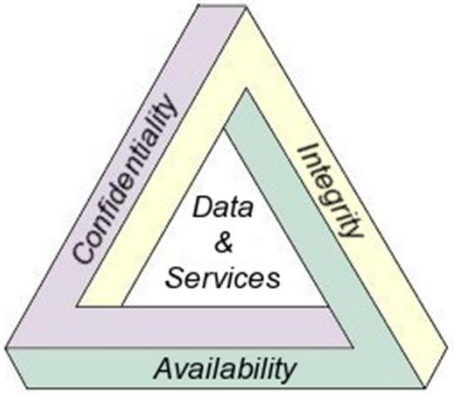
Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Qonnections

Global Partner Summit 2010

MIAMI

Information security
The CIA Triangle



Confidentiality
Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

Integrity
In information security, integrity means that data cannot be modified without authorization.

Availability
For any information system to serve its purpose, the information must be available when it is needed.

QlikView in the CIA Triangle

- **Confidentiality**
  Securing data is an important part of your role as an QlikView consultant. For this we have tools such as Publisher, QVS and Section Access.

- **Integrity**
  QlikView never alter or adds the source data, only read from it.

- **Availability**
  This is QlikViewôs main goal, making data available but secure.

  What is the point storing data if you canôt use it?

Qonnections

Global Partner Summit 2010

MIAMI

The Chain Is No Stronger Than Its Weakest Link

- We must have the same or better security in QlikView as the data source that we are loading from!
- Secure your connection strings
- Allowing QlikView Application downloading is a potential security threat. Use QlikView Server.
- QVW files are only secure when behind a QlikView Server
- Never disregard security at a customer site!

Qonnections

Global Partner Summit 2010

MIAMI

Communication with IT and security experts

- This presentation is created from field experience.
- Communication with IT and security departments is crucial for QlikView growth in big accounts.
- The customers IT departments and end users must have confidence in our security solutions.
- What you learn now will (hopefully) improve your credibility when talking QlikView and security.
- Our historical weak point in security focus, will be our strength!

Qonnections

Global Partner Summit 2010

MIAMI

Components in QlikView 9

Product Overview

QlikView Developer

- Development tool to create data model and graphical interface

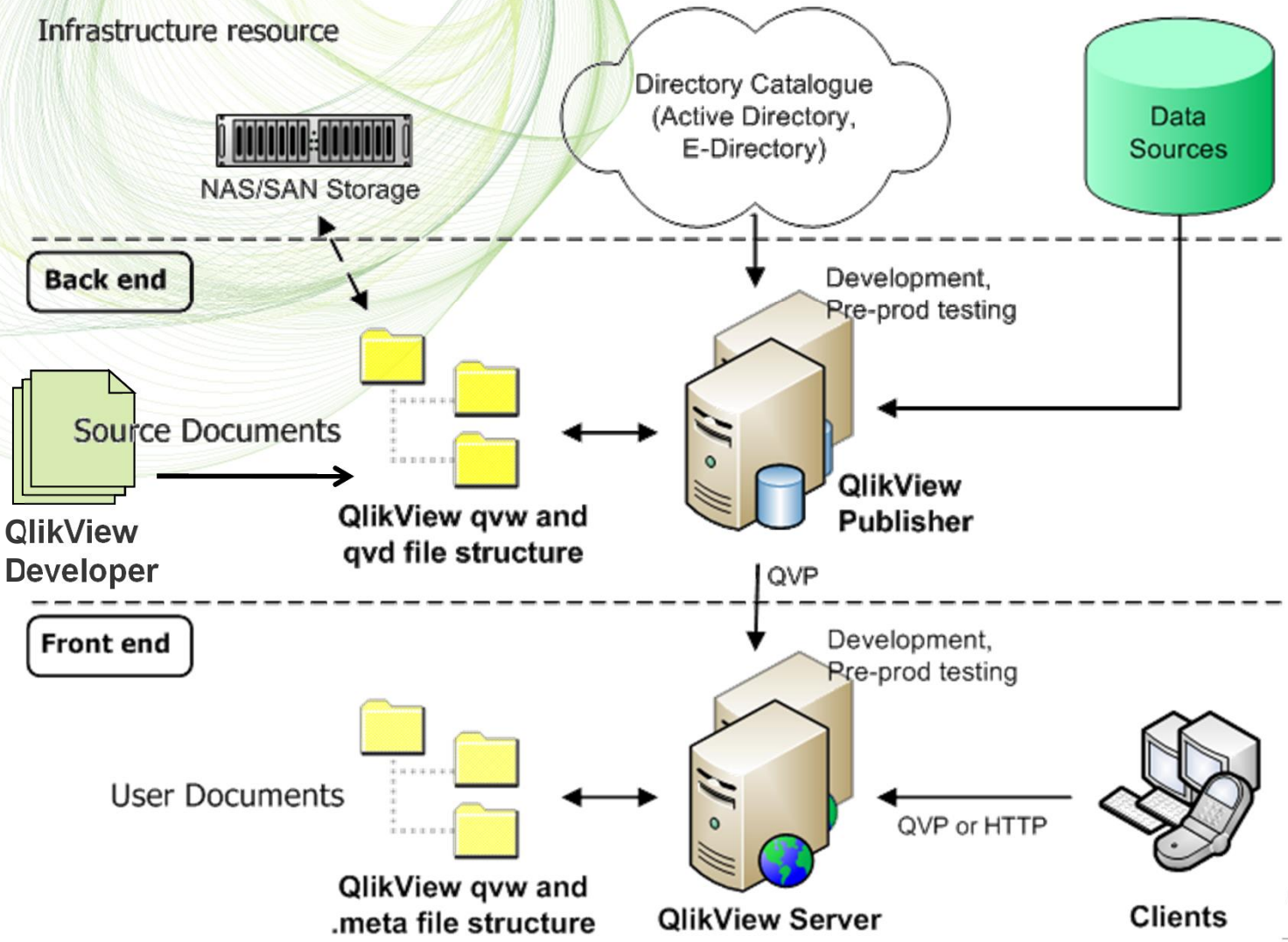
QlikView Server (QVS)

- Handles QlikView Client/Server communication
- Client Authorization against directory providers (AD, eDirectory..)
- Reads security ACL on qvw documents (NTFS or DMS)
- Writes security ACL on qvw documents (NTFS or DMS)

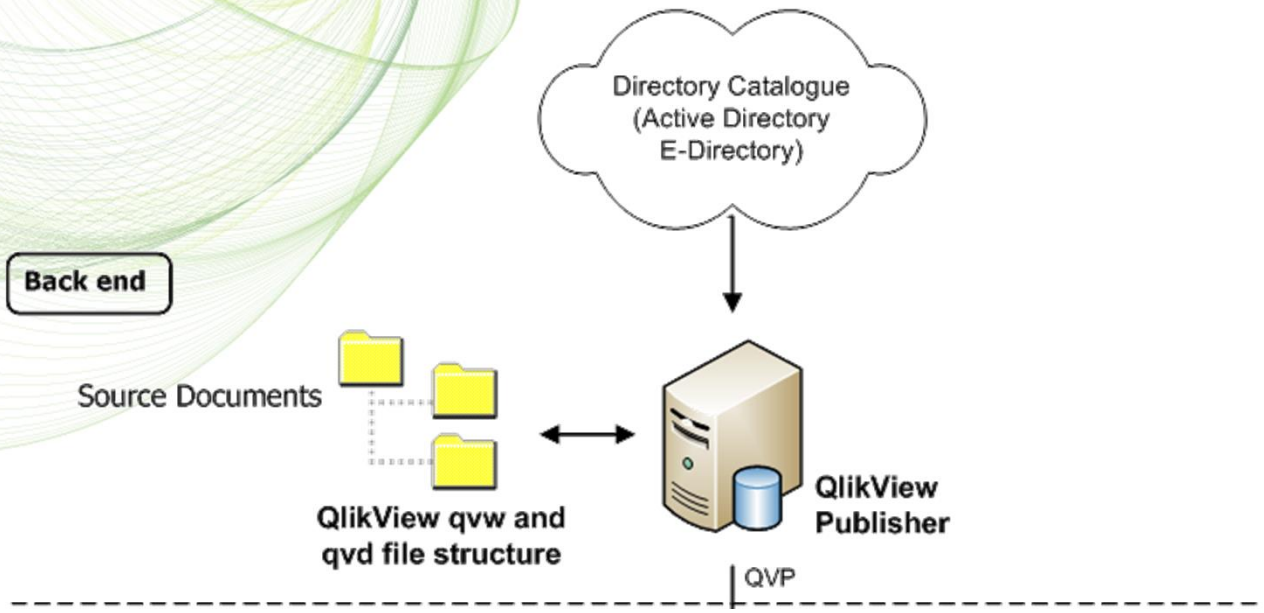
QlikView Publisher

- Load data from data sources
- Reduce applications depended on rules
- Lookup users and/or groups from directory providers
- Distribute qvw documents to a QlikView Server

Where do the QlikView products fit in?

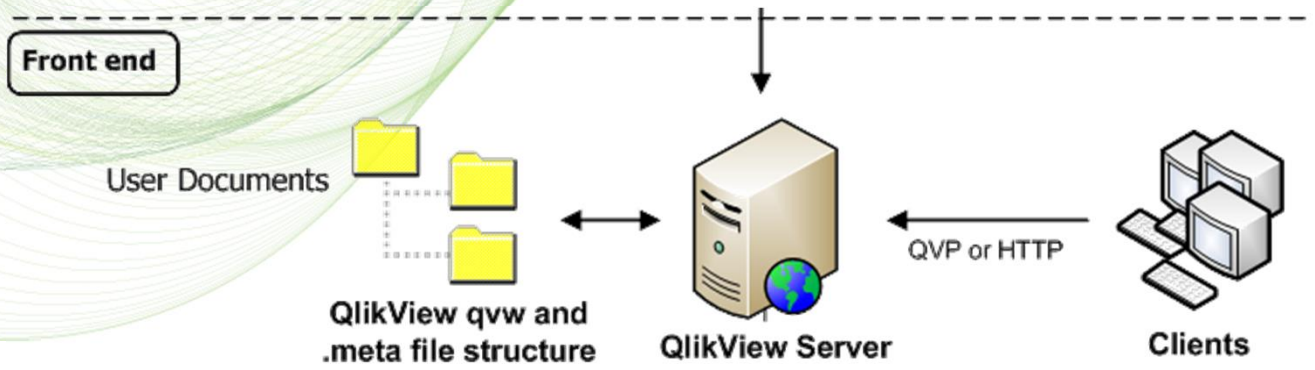


QlikView architecture, Back-end



- Contains QlikView *Source Documents* created by QlikView Developer
- QlikView file types are QVW, QVD and .log (if log active)
- The Windows file system is always in charge of security.
- QlikView Publisher is the main component in the back-end

QlikView architecture, Front-end



- Contains *User Documents*, this is by the Publisher distributed documents.
- QlikView file types are QVW, .META and .SHARED
- QlikView Server (QVS) is in charge of client security.

Security bullets regarding back-end/front-end Architecture

- Back and front-end are often in different network zones
- The front-end does not have any open ports the back-end
- The front-end does not send any queries to data sources in back-end
- The end users can only access QlikView documents in the front-end, never in the back-end.
- One back-end publisher server could connect to several frontend QVS
- The QlikView documents in front-end are a result of Publisher tasks.
  - It does not contain any overhead or redundant data (or should not)
  - It does not contain any connection strings
  - To recreate all the qvw documents just run the Publisher tasks
- These are all important QlikView security ñfeaturesò

Qonnections

Global Partner Summit 2010

MIAMI

Back-end security

Folder and security structure

- Why the need for a common file structure in back-end?
- File structure example
- File security in back-end.
- Securing your data sources

QlikView and multiple environments

- How to design a multiple environment
- QlikView in a multiple Environment bullets

Publisher and distribution

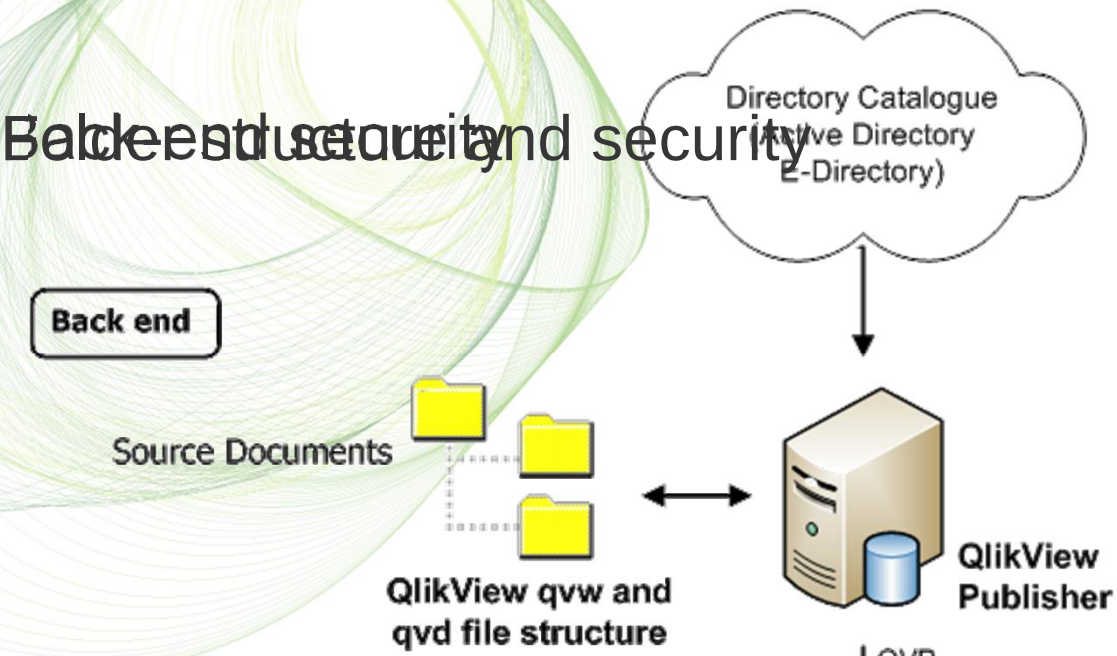
- Architecture components walkthrough
- Distribution process flow
- QlikView Publisher Directory Service Connector

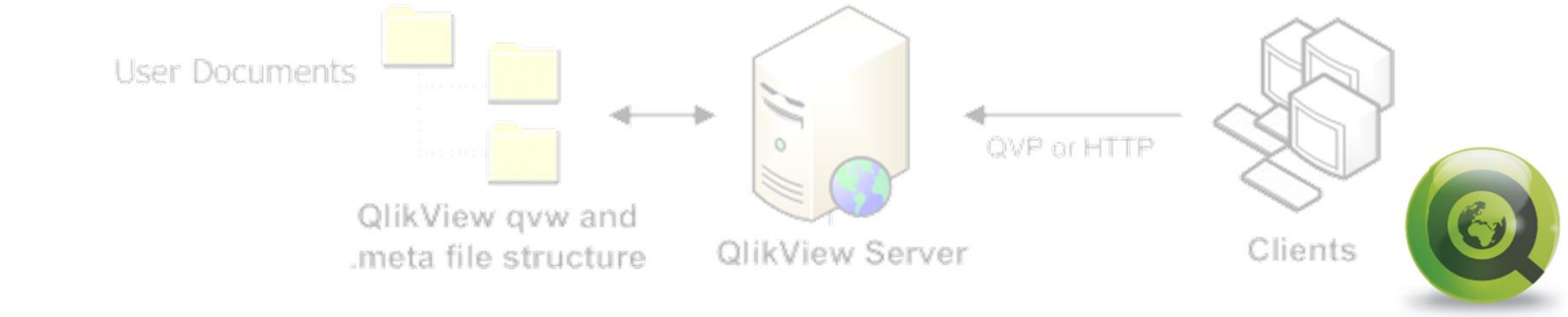
Qonnections

Global Partner Summit 2010

MIAMI

Back end security





Qonnections

Global Partner Summit 2010

MIAMI

Folder and security structure, Overview

- Design and document a folder structure for QlikView source files, depending on your customer needs, example later
- Design and document a security structure for your QlikView source files based on the folder structure, example later
- Always use relative paths in QlikView scripts
- Always use include files for data connection strings (ODBC/OLEDB) Placed according to the folder structure guideline.
  $(Include=..\include\DBserver_database.txt
- Use include files for common functions like inline tables and variables
- Create a QlikView Document template with your graphical company profile.
- *A good idea is to have predefined Include files with variables in the template*

Qonnections

Global Partner Summit 2010

MIAMI

Source folder structure Example

This is an example how to structure the QlikView Source files.

Have separate folders for

Departments, QVD files, include files and Script files

Department1\Applications	
QVD-files	QlikView documents (qvw) including subfolders
include-files	QlikView data files (qvd) including subfolders
Scripts	include files, connection strings and inline tables
Config	Special publisher scripts
Department2\Applications	Configuration files (shared folder), xls, txt, mdb é
QVD-files	
include-files	
Scripts	
Config	
Common_folders\Applications	QlikView common documents (qvw)
QVD-files	QlikView common data files (qvd)
include-files	Common include files, connection strings
Scripts	Special publisher scripts.
Config	Common configuration files

Qonnections

Global Partner Summit 2010

MIAMI

File security in back-end

This is an example how to secure your QlikView Source files.

Use domain security groups to match your source document file structure

A. Group for Departement 1 or Development A
   Change permissions only

B. Group for Departement 2 or Development B
   Change permissions only

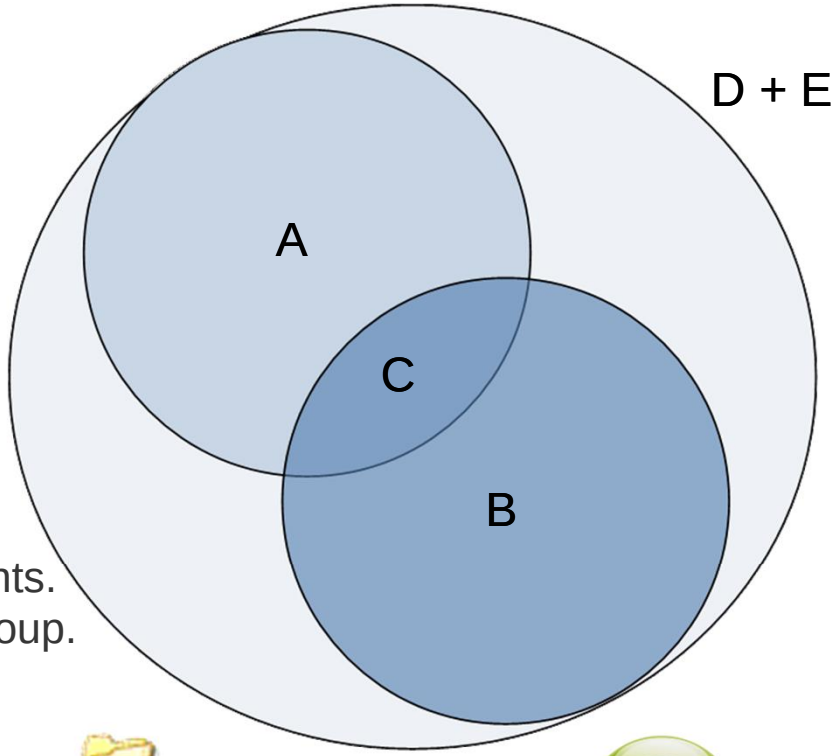
C. Group for Shared company data,
   Containing group A and B

D. Domain level QlikView Administrator group
   has access to all groups and distributed documents.
   Should also be member of the local QV admin group.

E. The Service Account for QlikView service,
   are member of group **D**

The Service Account must have access to:

- File system
- Active Directory
- Databases (for SQL SSO)



D + E

A B C
D + E D + E D + E

Qonnections

Global Partner Summit 2010

MIAMI

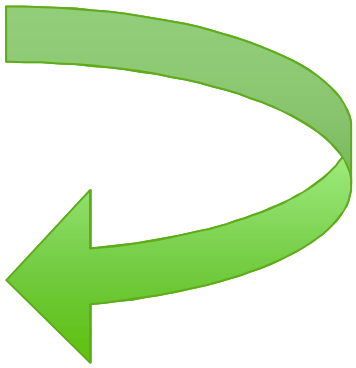
Securing your data sources

- By removing the development groups security rights on the *include-files* folder only the domain level *QlikView Administrator* group and Publisher will have rights to read and write the connection string.
  Department1\include-files

- To add an extra data security layer, create a separate folder structure containing qvd loaders for your data bases. Copy cleansed qvd files to the *QVD-files* repository in each department, SAP example:

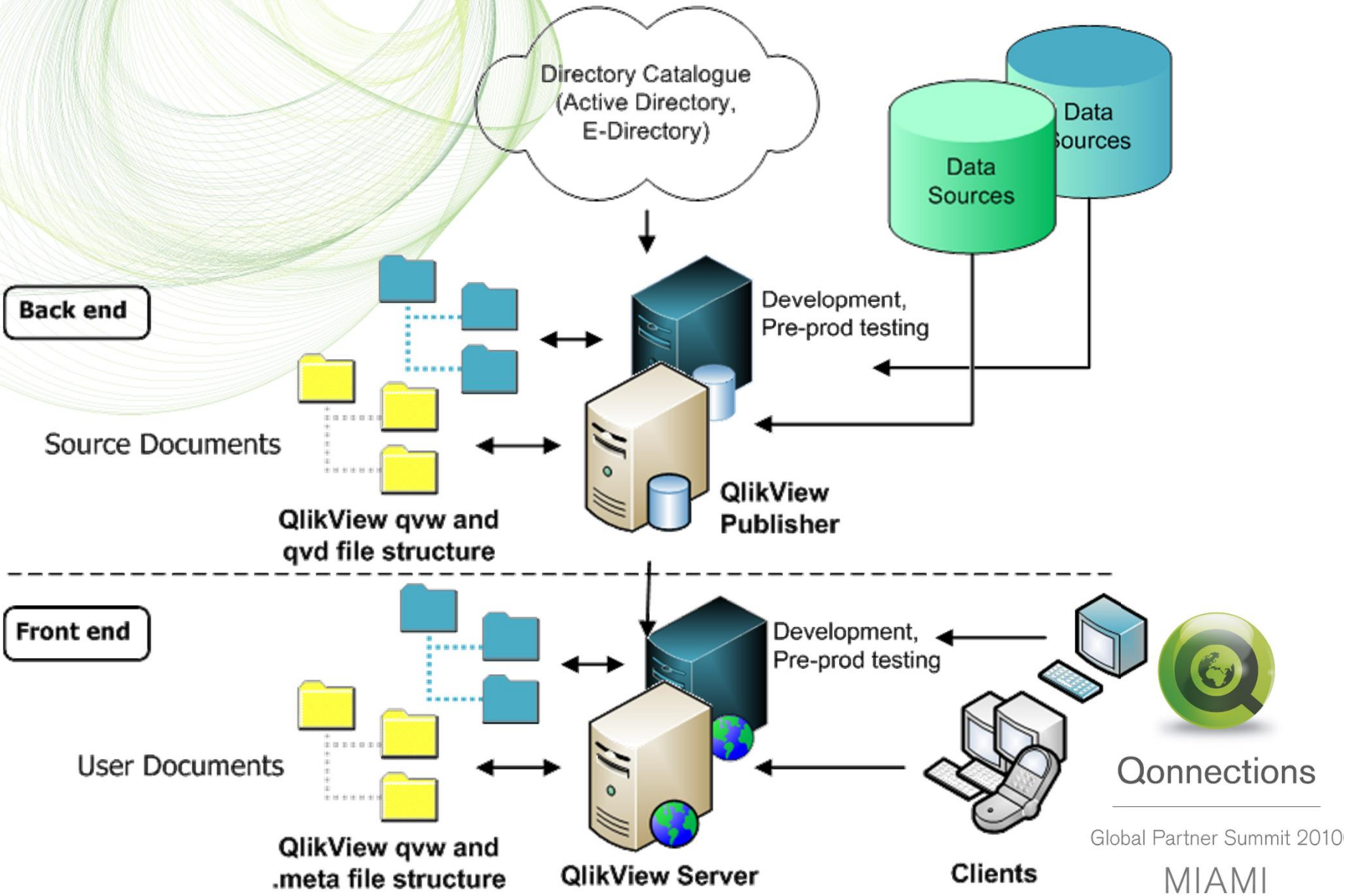
SAP\Applications\QVD-Loader.qvw
include-files
QVD-files
Department1

Department1\Applications
QVD-files
SAP-data



Qonnections
Global Partner Summit 2010
MIAMI

QlikView and multiple environments



Qonnections

Global Partner Summit 2010

MIAMI

QlikView in a multiple Environment, bullets

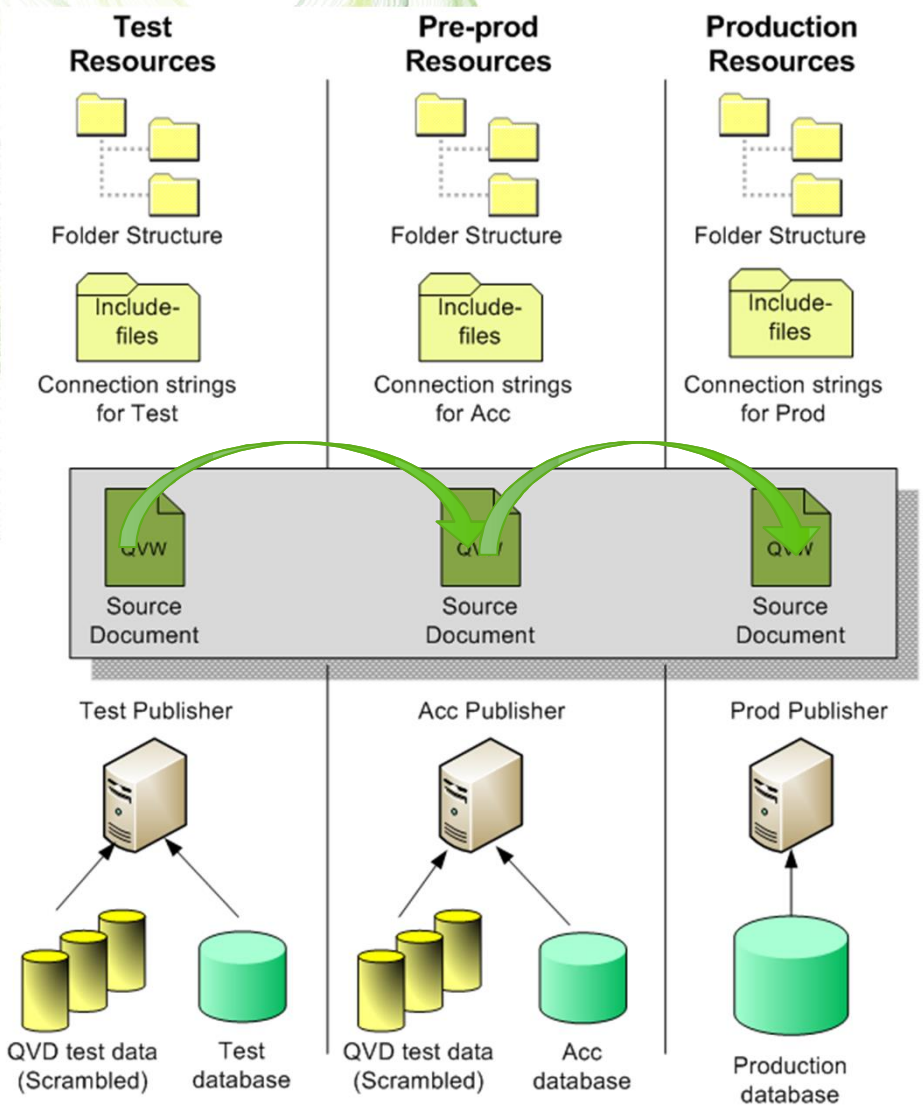
- The document folder structure in each environment should be identical
- Servers in the environments do not need to have the same hardware specs. Use VM when needed.
- When moving applications between the environments QlikView documents will automatically connect to different data sources depending on the connection string in the include folders
- This procedure will require that the databases for test and pre-prod are equivalent to the production databases
- In lack of good test data a work around is to create scrambled QVDs from production and use as test data. Use include-files for qvd loading.

Qonnections

Global Partner Summit 2010

MIAMI

How to design a multiple environment

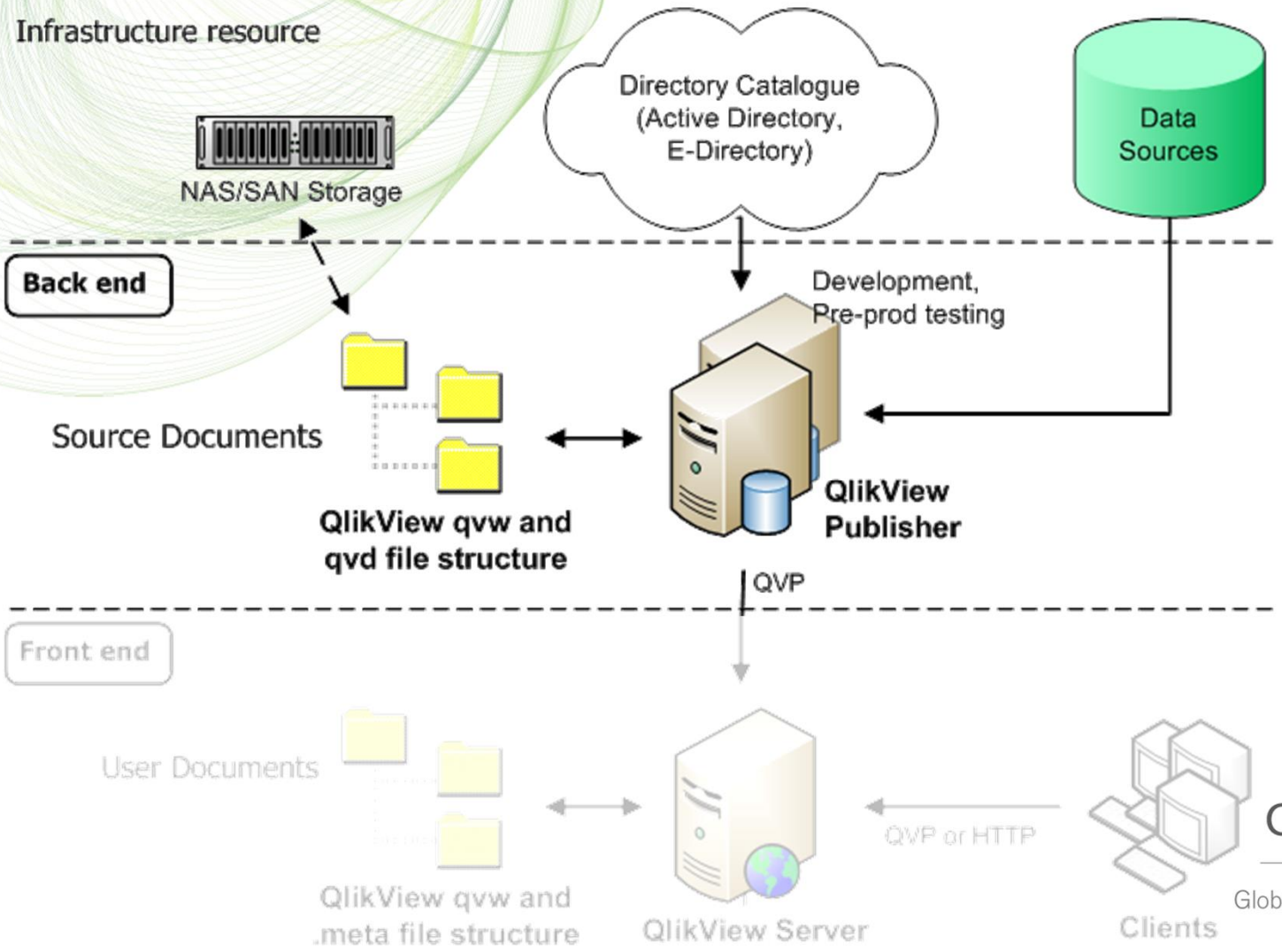


Qonnections

Global Partner Summit 2010

MIAMI

Publisher and distribution

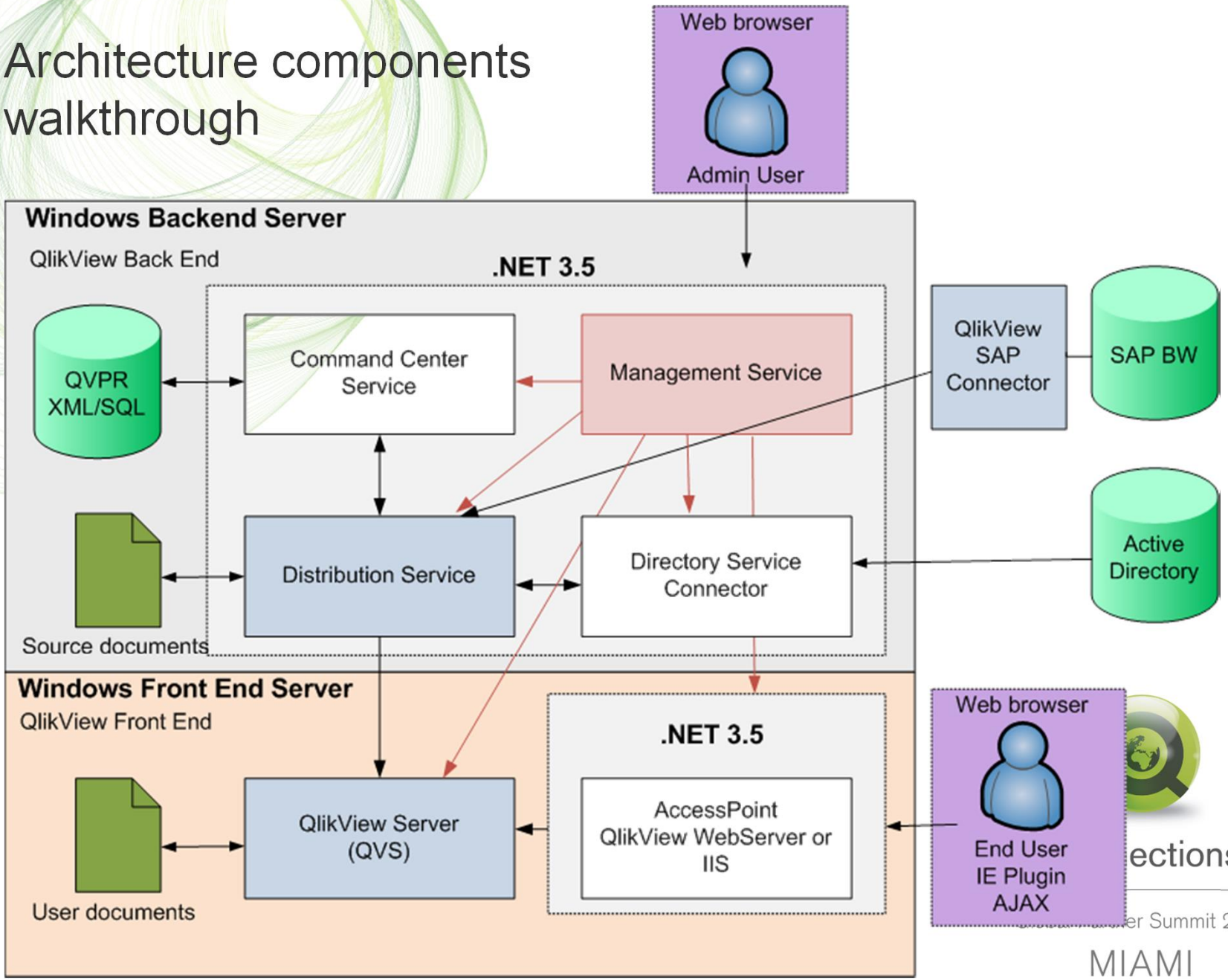


Qonnections

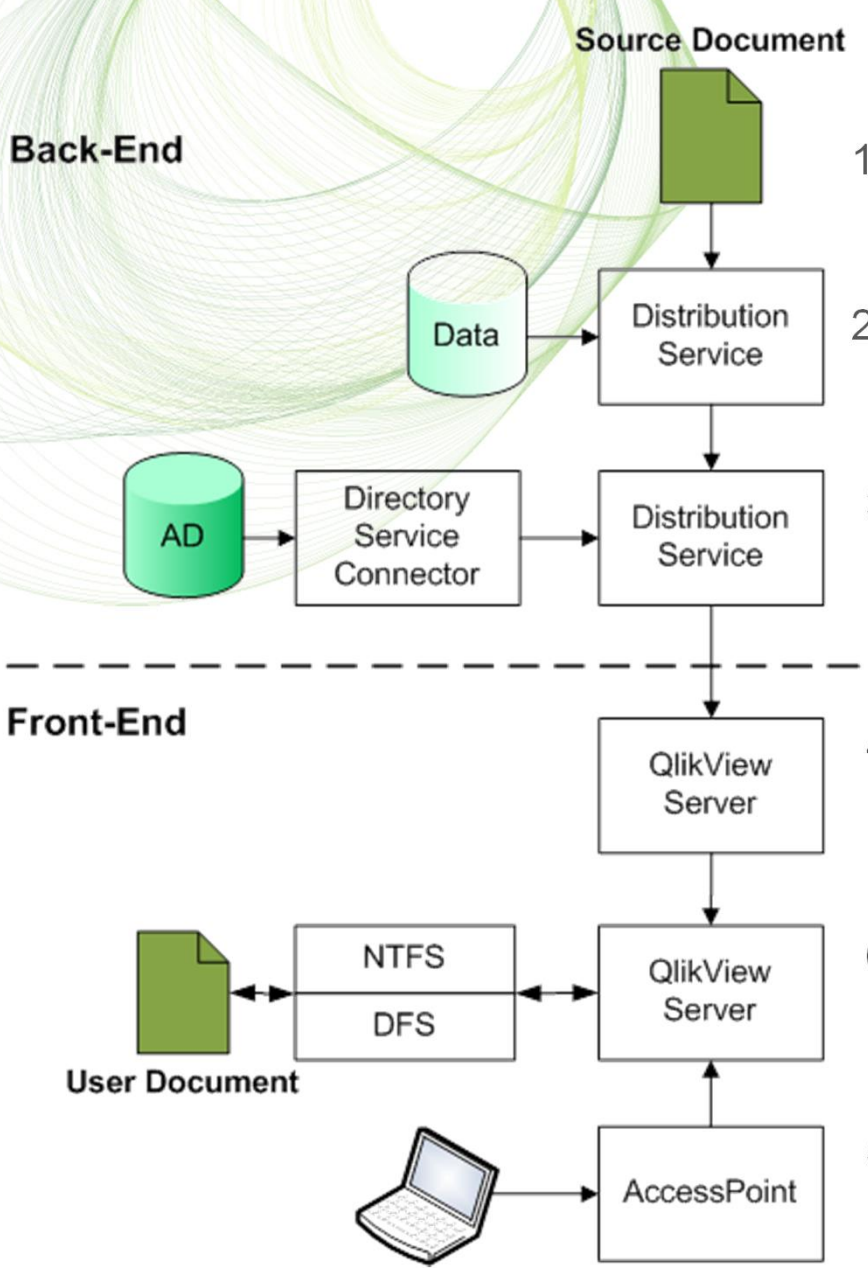
Global Partner Summit 2010

MIAMI

Architecture components walkthrough



QlikView loading and publishing Workflow



1. QlikView document from a developer.
   Resides in source document file structure

2. Reload Stage:
   Load data from databases.

3. Distribution Stage:
   Reducing data
   Looking up security from AD via DSC
   Distributing to QVS (port 4747).

4. QVS sets security right given by QDS and saves the document.

6. QVS checks what documents end user have access to.

5. End user logs in to AccessPoint.

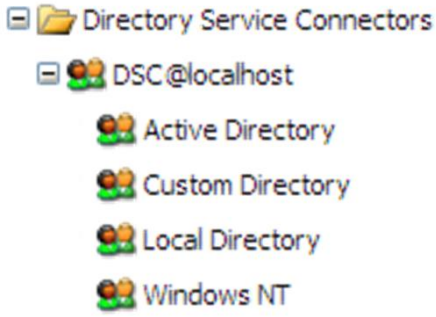
Qonnections

Global Partner Summit 2010

MIAMI

QlikView Publisher Directory Service Connector

- QlikView Directory Service Connector (DSC) is the security service in Publisher. Itôs task is to lookup users and groups from a directory source.
- DSC have plug-in modules to directory sources, They are called Directory Service Providers (DSP)
- Default modules are:
  - Active Directory
  - Custom Directory (Custom Users)
  - Local Directory (Local Users)
  - Windows NT Legacy (Samba)



- SDK and xml provider example is available for custom DSP creation
- Custom DSPôs works together with DMS mode on QlikView Server
- QlikView have a Custom DSP for Novel
- Remember there is no QlikView support for custom DSP modules (except the APIôs)

Qonnections

Global Partner Summit 2010

MIAMI

Questions regarding Back-end security?

Highlights

- Separate the Back-End and Front-End environments
- Protect your customers data and data sources
- Design and document a folder structure for QlikView source files
- Secure your QlikView source documents by using security groups in Windows.
- Try to use multiple environments at customer site
- Always use relative paths in QlikView scripts
- Always use include files for connection strings
  $(Include=..\include\DBserver_database.txt

Qonnections

Global Partner Summit 2010

MIAMI

Front-end Security

Qonnections

Global Partner Summit 2010

MIAMI

Front-end Security

Front-end security overview

- QlikView Server default security
- Windows NTFS or DMS mode
- DMS population methods
- QlikView Server communication protocols (QVP and QVPX)

QlikView Server Authorization

- Ticket exchange
- Single Sign On (SSO) using HTTP header
- AccessPoint HTTP header security
- Reverse Proxy

Section Access

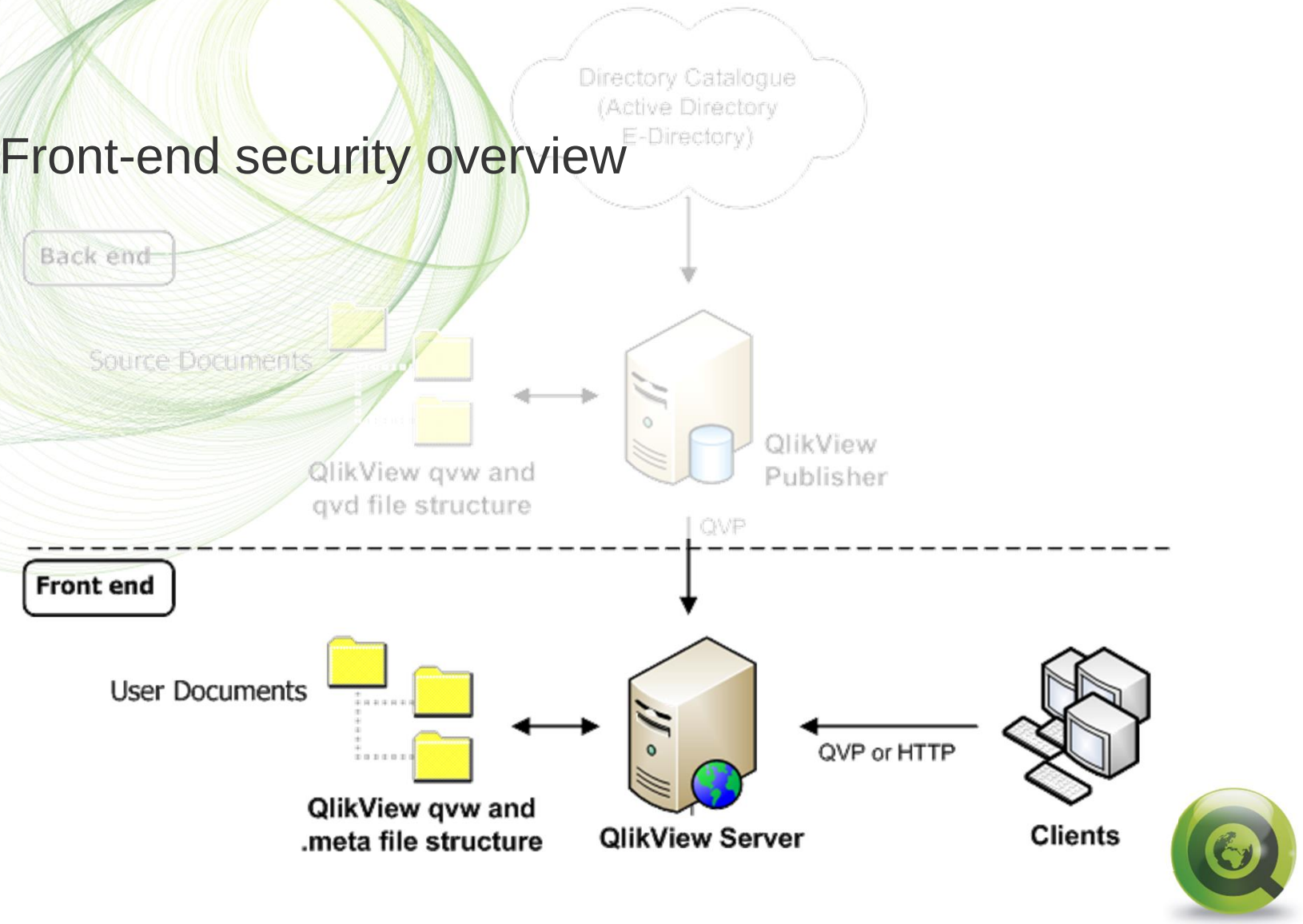
Questions

Qonnections

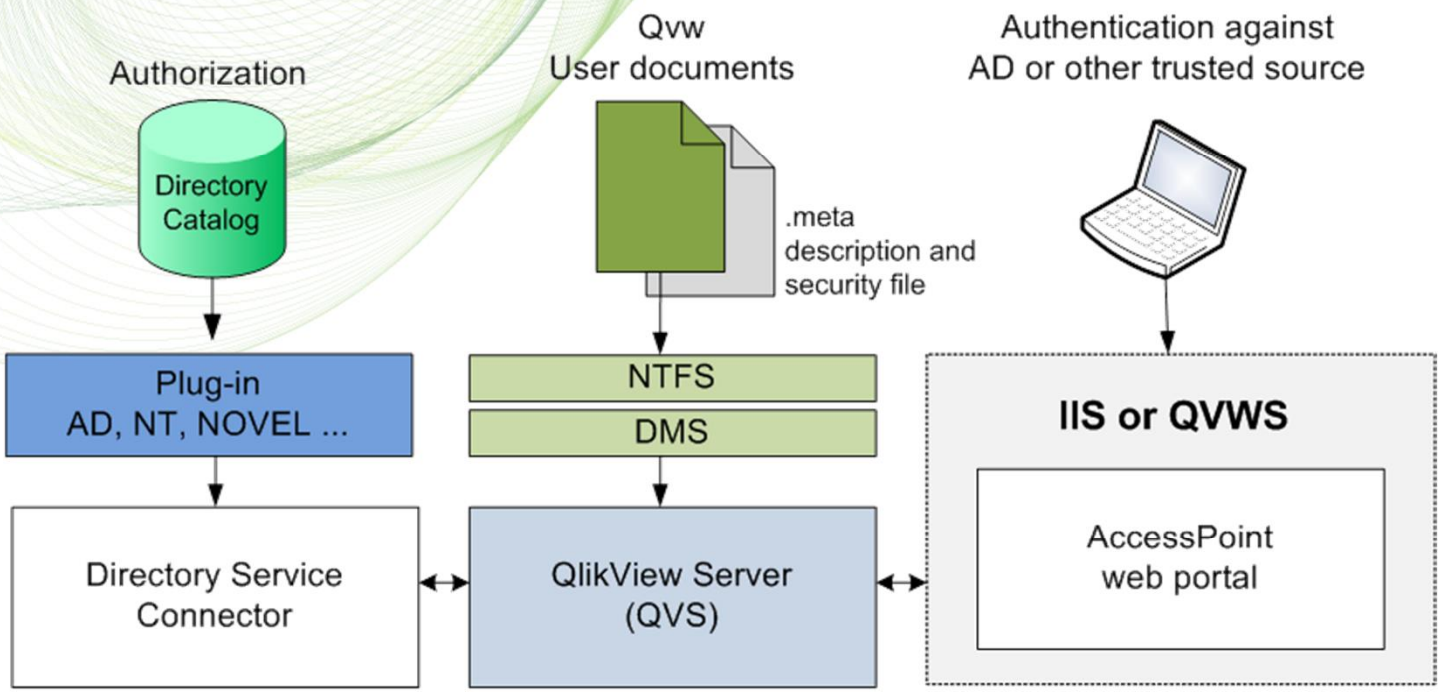
Global Partner Summit 2010

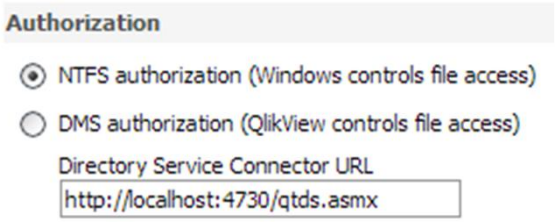
MIAMI

Front-end security overview



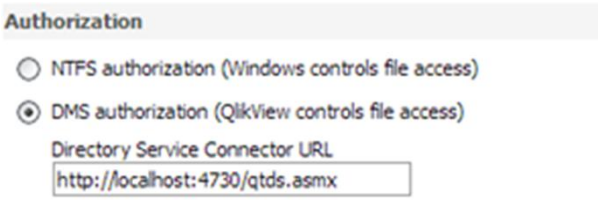
Front-end architecture components





QlikView Server default security (NTFS Mode)

- QlikView is fully integrated with Windows security.
- This means that Windows Authenticates QlikView users when logging in to Windows.
- QlikView validates (authorization) the already logged in user against Windows. Security mechanism is Kerberos or NTLM.
- QlikView Server writes user and group access on the QlikView documents with NTFS ACLs.



DMS security

- When using DMS mode the ordinary Windows NTFS security in QlikView Server will not be used.
- Instead of writing ACLs on the QlikView file a .meta file will be attached to the user documents. The Meta file will include user and/or group access for the qvw file it represents.
- You can still use AccessPoint Windows authorisation with DMS
- QlikView Server will authorize the Meta file users against a trusted directory service or website.
  Example of a DMS directory source is Novel eDirectory.

DMS Population Methods

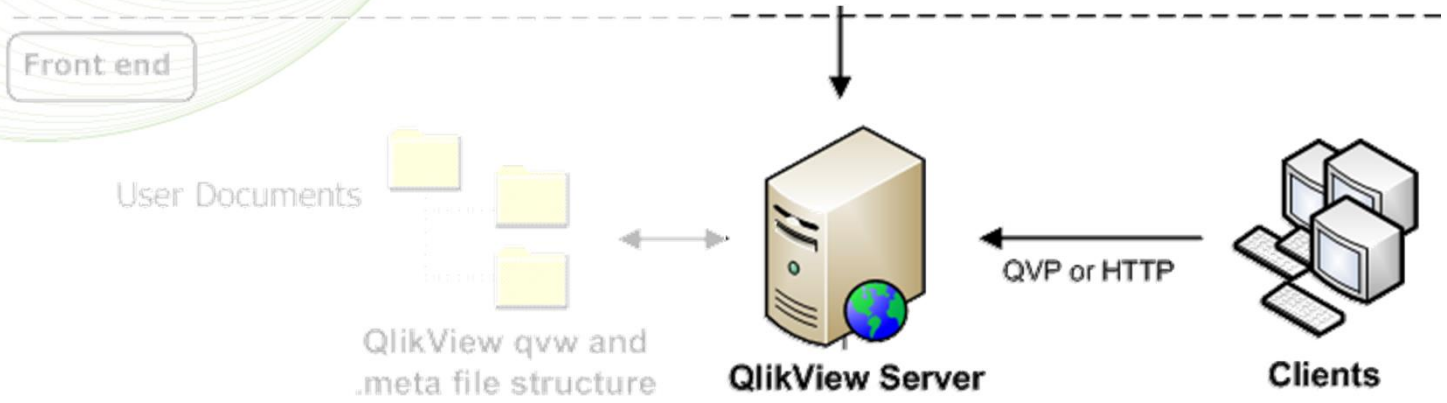
- Enter manually in the Management Console
- QlikView Publisher writes DMS users and groups via QlikView Server. This is done by the Directory Service Connector (DSC) and DSP plug-ins for directory sources.
- Programmatically using APIs (DEMO)

Qonnections

Global Partner Summit 2010

MIAMI

QlikView Server communication protocols
QVP and QVPX



Qonnections

Global Partner Summit 2010

MIAMI

QlikView Server communication protocols
The QlikView Protocol (QVP) Overview

- QVP is a proprietary protocol developed by QlikTech.
- The protocol lays down a specification for passing data between QlikView Server and installed clients, like QlikView Plug-in and Developer open in server.
- QVP runs natively over TCP port 4747 or may be encapsulated over HTTP by use of the QVP tunnel.
- QVP only transports screen updates and this in binary code.

Qonnections

Global Partner Summit 2010

MIAMI

QlikView Server communication protocols
The QlikView Protocol (QVP) Security

- Authentication: The QVP uses the mechanism in Windows (Kerberos/NTLM) to authenticate the client to the server before starting the QVP communication.
- Encryption: The Client generates a 128-bit public RSA encryption key. When a session is being established this key is sent to the QVS.
- Encryption: The server generates two random 128-bit session keys (one for each direction). These are encrypted with the public key from the client.
- Use QVS Tunnel and SSL for extra security.

Qonnections

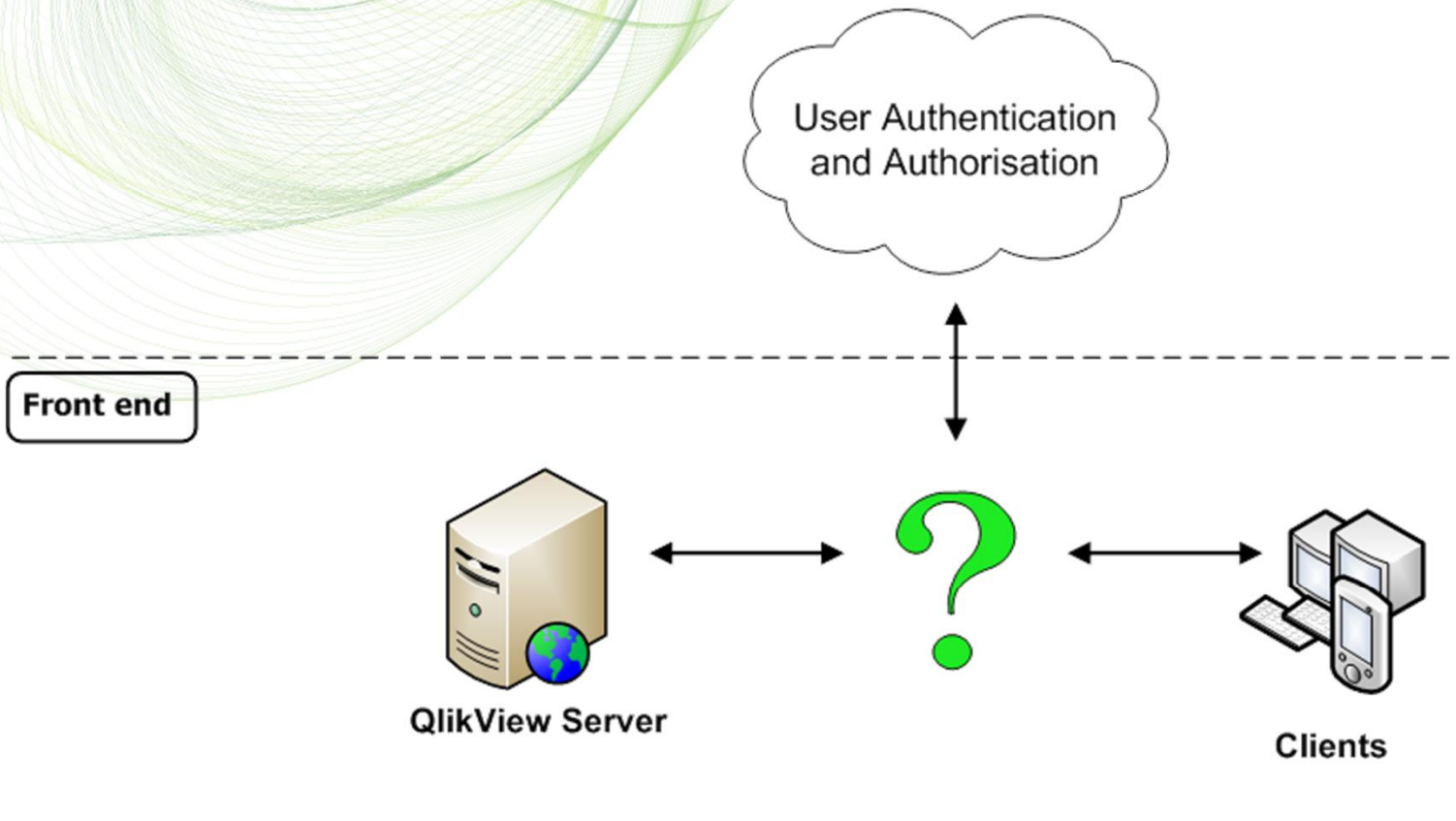
Global Partner Summit 2010

MIAMI

QlikView Server communication protocols
The QlikView AJAX Protocol (QVPX)

- QVPX is proprietary and developed by QlikTech.
- QVPX is used by the AJAX and mobile clients.
- This is not really a protocol, but rather a framework how QlikView communicates in AJAX (xml and Java Script).
- The actual protocol is HTTP or HTTPS.
- Encryption is done with certificates and SSL
- The advantages with QVPX is that HTTP/HTTPS is standard protocols well known and trusted by IT departments.

QlikView Server alternative authorization methods



Qonnections

Global Partner Summit 2010

MIAMI

QlikView Server authorization using ticket exchange

- To be granted access to a QlikView file in DMS mode a ticket exchange have to be performed.
- AccessPoint has the ticket exchange functionality built in.
- When Integrating a third party system like a web portal the ticket exchange could be used.

Qonnections

Global Partner Summit 2010

MIAMI

Ticket Exchange (DEMO)

1. User Bob logs in to a site (authentication) and wants to access QlikView.

2. A trusted site (usually the logon site) is requesting a ticket for Bob.

```
http://sesth-rfn/TicketExchange/index.asp?user=BOB
```

3. QVS creates a ticket and stores it together with the username in TicketData.pgo.

4. Ticket is returned to the requesting site.

```
<Global>
    <_retval_>
        338270F1A283D8925AEAAE5CE41B97DD353F6CDB
    </_retval_>
</Global>
```

The ticket is a 40 character hex hash with XML headers. You must strip off the XML headers before passing back to the QlikView Server.

5. Client uses the ticket to request the document.

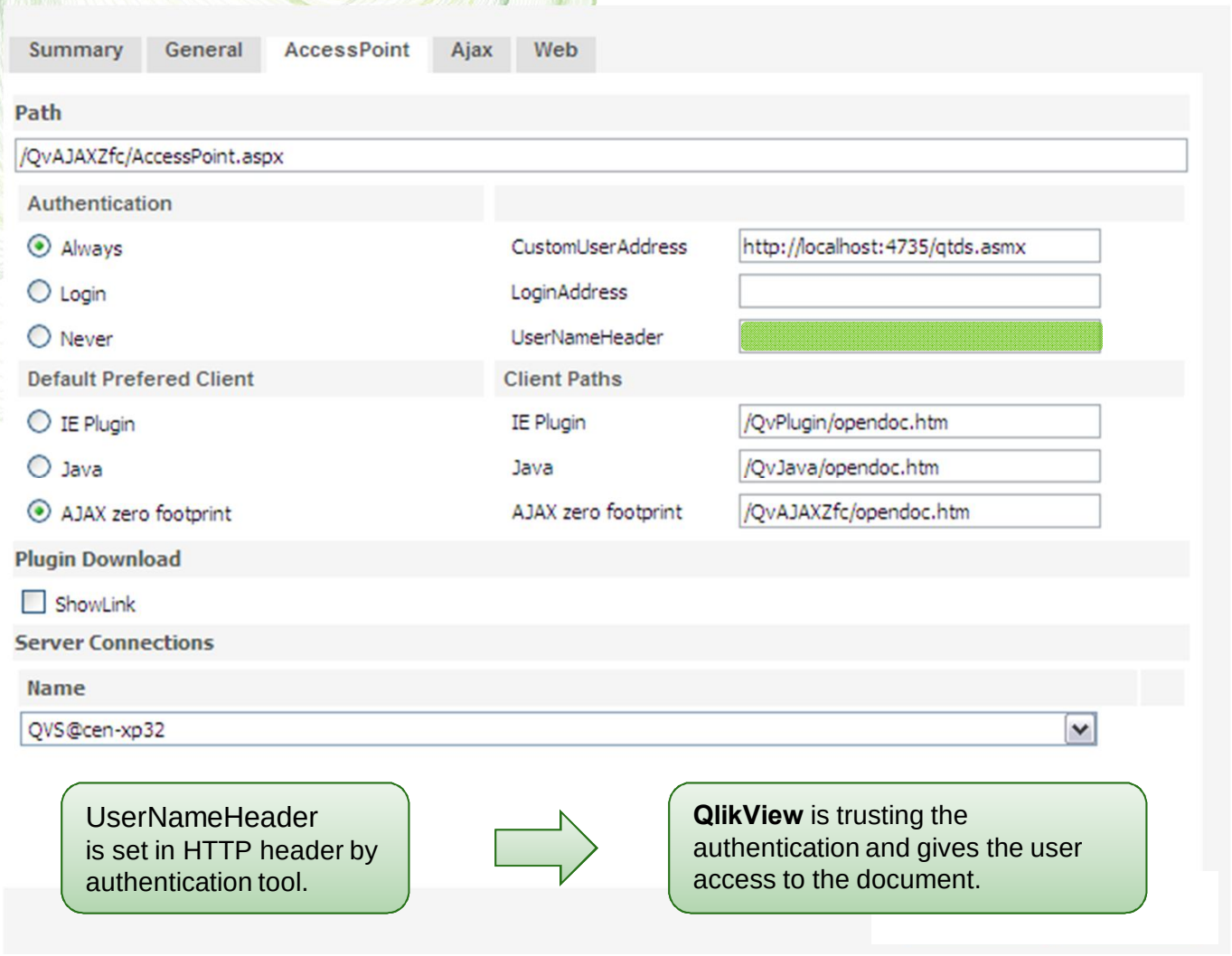
```
http://sesth-rfn/AJAX/default.htm?userid=338270F1A283D8925AEAAE5CE41B97DD353F6CDB
```

6. QVS checks ticket against the stored ticket in TicketData.pgo.

7. If ticket is OK then QVS retrieves the username.

8. QVS checks DMS metadata if user is authorized to view the document.

QlikView Server authorization using AccessPoint SSO (DEMO)



UserNameHeader
is set in HTTP header by authentication tool.

QlikView is trusting the authentication and gives the user access to the document.

Qonnections

Global Partner Summit 2010

MIAMI

AccessPoint HTTP header security

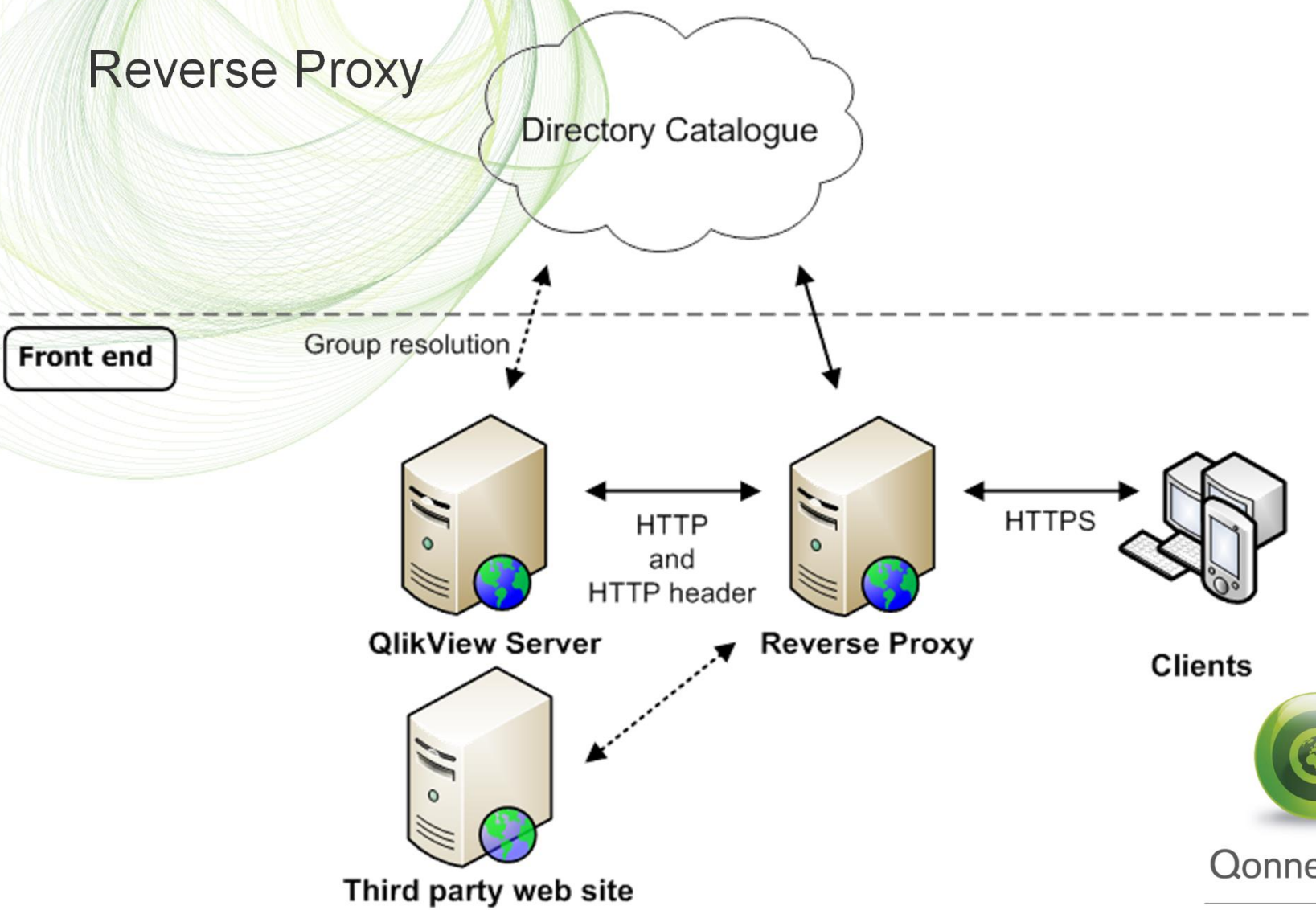
- Sending a HTTP header is not secure!
  AccessPoint using SSO with a header need to have additional security.
- Using SSO with SiteMinder. A ISAPI filter in IIS will act authorization provider.
- Third party hardware boxes can provide reverse proxy and authorisation functionality for AccessPoint. (Example is Mobility Guard)
- Using Reverse Proxy with an external web servers like Apache or IIS.
  But you still need a mechanism to set the HTTP header!
- Always use SSL encryption

Qonnections

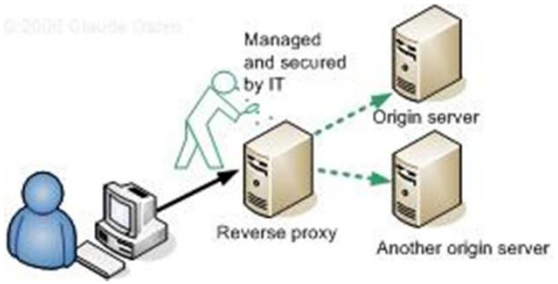
Global Partner Summit 2010

MIAMI

Reverse Proxy



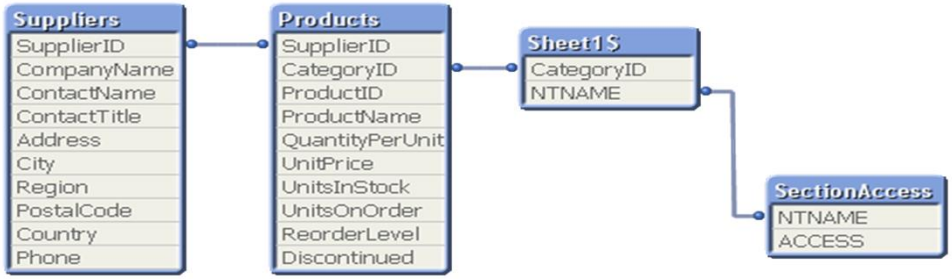
Reverse Proxy



- A reverse proxy is either a proxy server that is installed in a server network or a network equipment.
- Typically, reverse proxies are used in front of one or more Web servers.
- All connections coming from the Internet addressed to one of the Web servers are routed through the proxy server.
- Reverse proxies provide an additional layer of defense by masquerading the web server behind the proxy.
- Reverse proxies can also provide Application firewall features, to protect against common web-based attacks.
- Secure Socket Layer (SSL)

Section Access (DEMO)

```
Section Access;
LOAD * INLINE [
ACCESS, NTNAME
ADMIN, MBG
ADMIN, QTSEL\MBG
USER, JOHN
USER, BEN
USER, LISA
USER, SANDRA
USER, BOB
];
Section Application;
```



Qonnections

Global Partner Summit 2010

MIAMI

Section Access Overview

- Section Access is not secure when downloading, use QVS!
- Section Access security is set in the script.
- Section Access can be used to set access restrictions to data, sheets and sheet objects.
- All access control is managed in the same way as QlikView normally handles data. Section Access is a part of the application data model.
- For QVS SSO login with Section Access use *ACCESS*, *NTNAME* fields in the script. Works in both NTFS and DMS mode.
- *ACCESS* = *ADMIN* for developers (concatenated inline + include)
  ACCESS = *USER* for users, usually loaded from a security data source
  Use string function upper() when loading.
- The system functions *OSuser( )* returns the current logged in username.

Qonnections

Global Partner Summit 2010

MIAMI

Highlights and Questions regarding front-end security?

- QlikView is fully integrated with Windows security. This is the default setting.
- When using DMS mode the ordinary Windows NTFS security in QlikView Server will not be used.
- QVP protocol is used by Plug-In and QVPX is used by AJAX and mobile client.
- Use SSL to secure your client/server communication.
- Sending a HTTP header is not secure! AccessPoint using SSO with a header need to have additional security.
- Section Access is not secure when downloading, use QVS!

Qonnections

Global Partner Summit 2010

MIAMI