Application Server Controlled Resources (ASCR)

ASCR is applied to Enterprise deployments where interactive clients are connected via Blue Prism application servers. Application Server Controlled Resources (ASCR) streamlines connectivity and increases the number of runtime resources that can be deployed in a single Blue Prism environment. ASCR allow organizations to deploy more than twice the number of digital workers into a single Blue Prism environment compared to Blue Prism version 6.

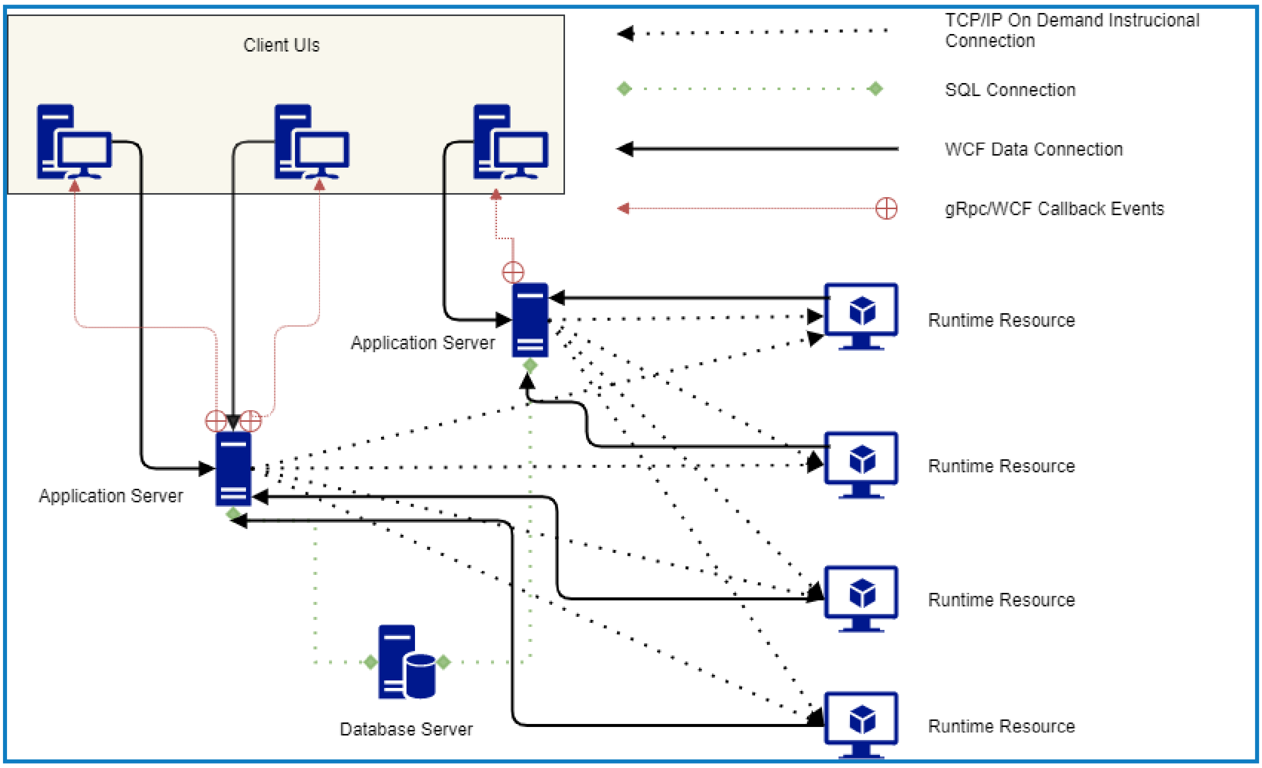
Architecture

ASCR is used automatically when the following conditions are met:

- Blue Prism version 7.0 or later is installed.
- Interactive clients are connected via Blue Prism application servers.
- The Blue Prism application server is configured to support callbacks – this configuration is mandatory. See ASCR server configuration for details.

Application server controlled resources

With ASCR, interactive clients communicate with available runtime resources via an application server, meaning that individual connections from each interactive client to each runtime resource no longer need to be made. This increases efficiency and enhances the potential for greater scale. ASCR uses connections on demand, connections are established, used and terminated as needed. Previously, connections were held open permanently.



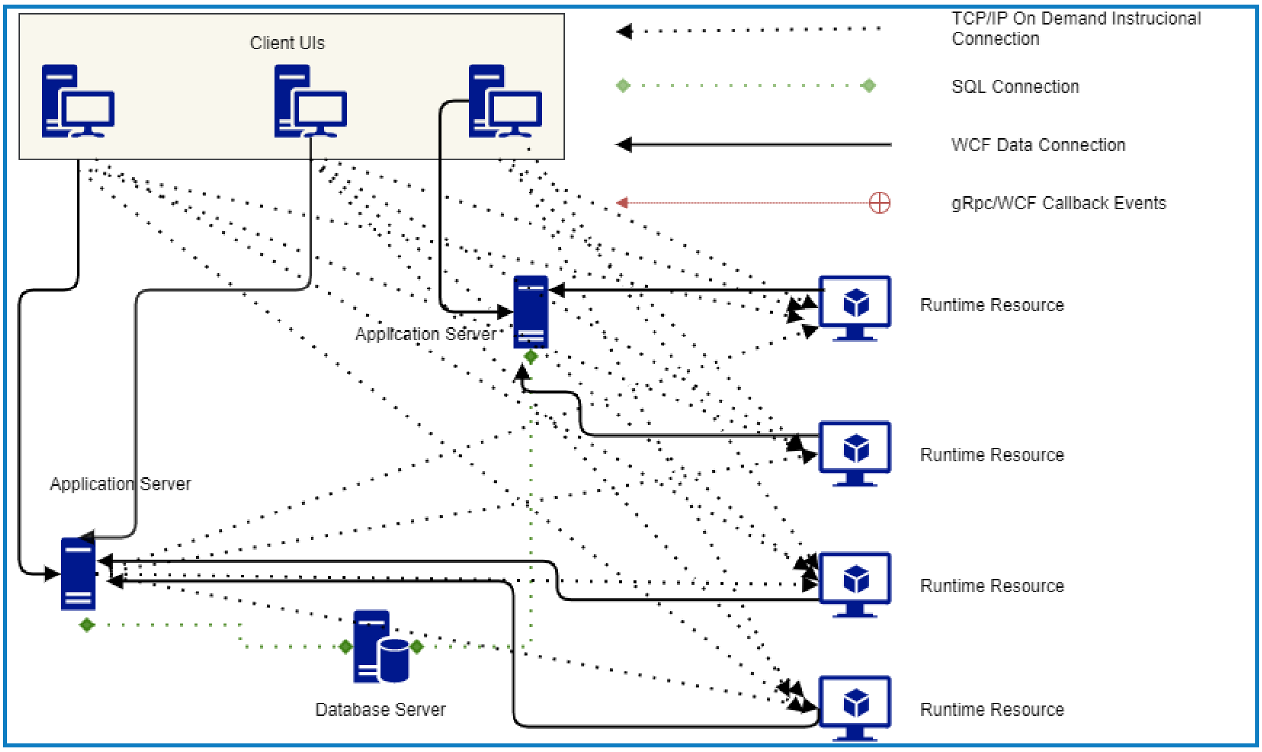
An event channel (gRpc/WCF bi-directional events in the diagram above) enables the client UI to receive updates from runtime resources in near real time. For example, when a session starts on a runtime resource, a *session started* event is sent to all connected services. With ASCR, this is only sent to the application servers. The callback channel enables such events to be forwarded to all connected client UIs. This enables the Control Room to update in near real time, without the need for the client UI to be directly connected to each runtime resource in the environment.

Blue Prism application servers and interactive clients must meet the specified minimum requirements, depending on the selected callback protocol, in order to successfully operate ASCR functionality.

Interactive client controlled resources

The following diagram shows the Blue Prism version 6 architecture. All interactive clients have connections to all available resources. This uses system resources both when creating and refreshing the connections; and when utilizing those resources.

This method is still used in Blue Prism version 7 if interactive clients are making a direct database connection.



ASCR server configuration

Interactive clients no longer have direct connections to each runtime resource when operating with application server controlled resources, however, there is some information that needs to be passed back from runtime resources in a timely manner. For this purpose, a new callback connection is established by each interactive client with its application server to allow this information to be passed back. After the client has established a connection with the server, it downloads the callback information specified on the server, and uses it to establish a secondary connection which the server uses for this purpose.

This section describes how to set up the callback connection in the application server configuration, which is referenced by Automate.config. This configuration can be set in the following ways:

- ASCR configuration via BP Server
- ASCR configuration via command line

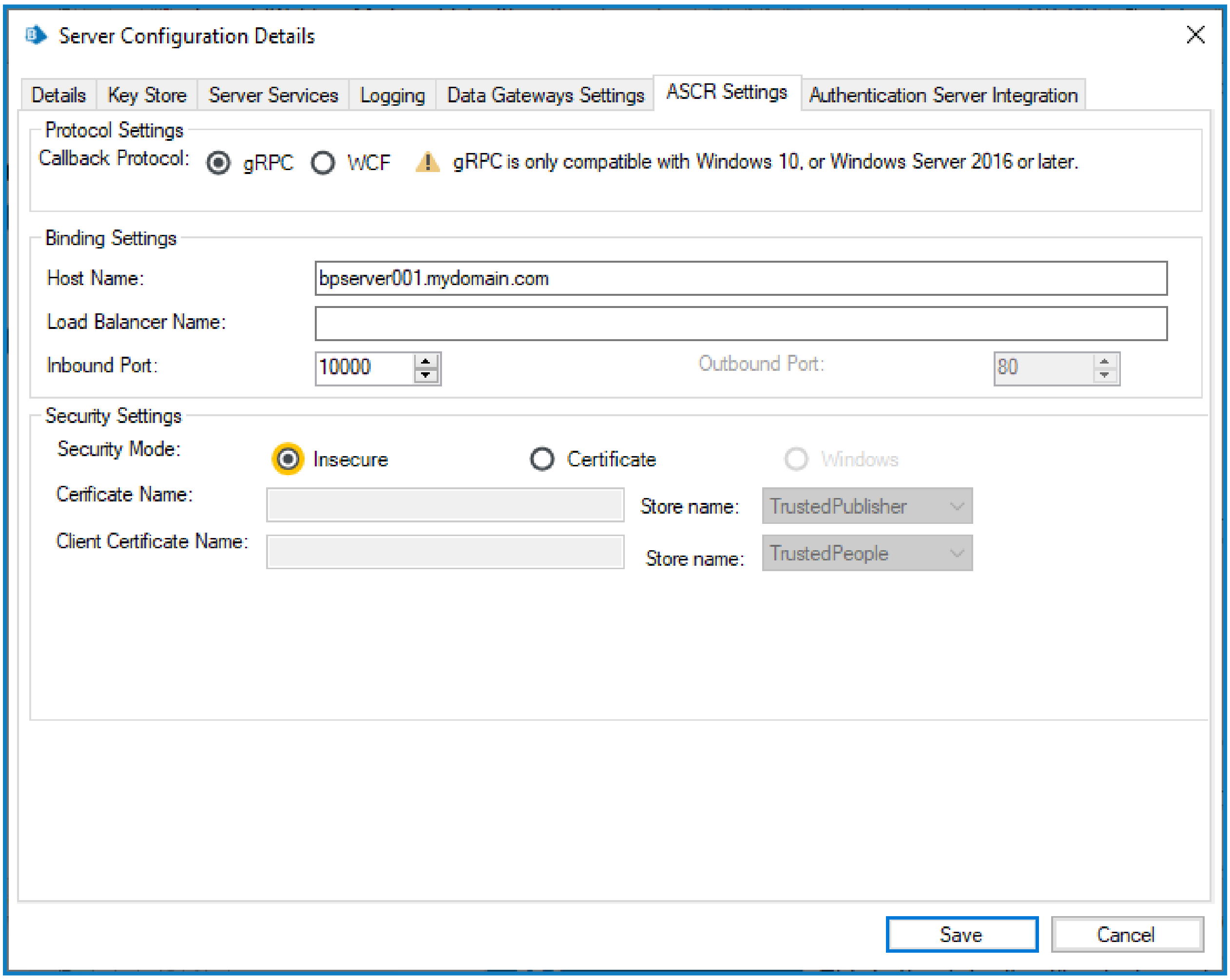
> The ASCR settings are applied to all interactive clients that connect via an application server with Blue Prism version 7. When upgrading a Blue Prism application server from version 6 to version 7, the server console output will display a message informing the user that the security mode cannot be *none*. This is to ensure the ASCR settings are configured, as described below.

For guidance on the troubleshooting of potential issues that users may encounter when using ASCR including ASCR logging, connections, and load balancing, see ASCR troubleshooting and logging on page 11.

ASCR configuration via BP Server

This procedure shows how to configure ASCR in BPServer and must be carried out for all Blue Prism application servers.

1. Open the BPServer.exe. By default, this is located in `C:\Program Files\Blue Prism Limited\Blue Prism Automate` or possibly `C:\Program Files (x86)\Blue Prism Limited\Blue Prism Automate\` depending on your installation environment.
2. To open the server configuration, select the relevant environment from **Current configuration** and click **Edit**.
3. Select the **ASCR Settings** tab.



Protocol Settings

Callback Protocol: ● gRPC ○ WCF ⚠ gRPC is only compatible with Windows 10, or Windows Server 2016 or later.

Binding Settings

Host Name: bpserver001.mydomain.com

Load Balancer Name:

Inbound Port: 10000 Outbound Port: 80

Security Settings

Security Mode: ● Insecure ○ Certificate ○ Windows

Cerficate Name: Store name: TrustedPublisher

Client Certificate Name: Store name: TrustedPeople

4. In Protocol Settings, select the required **Callback Protocol** method from the following options:

gRPC	This is the default callback channel and requires HTTP/2. The application server and all interactive clients that connect to it must be running Windows 11, Windows 10, or Windows Server 2016 or later. ⚠ This is the recommended option.

WCF	This callback channel supports Windows 11, Windows 10 and Windows Server 2016 and earlier.
	⚠ WCF should only be used if gRPC cannot be used.
	If you select this option and the service login account is not a local administrator, you will need to run the commands below to grant the service login account user permissions to start the listener using the default port settings:
	If the ASCR host name is blank, use the following command, which contains a wildcard:
	`netsh http add urlacl url=http://+:80/bpinstruct user=<domain>\<user>`
	If the ASCR host name is explicit, use the following command and include the host name:
	`netsh http add urlacl url=http://<fqdn>:80/bpinstruct user=<domain>\<user>`
	For either of these commands, the client inbound port number should be used. The examples above show the port number as 80, which is the default port. If you are using a different port, you must enter the correct port number.

5. Under Binding Settings, enter the **Host Name** for the channel to bind to.

   This is the host name of the application server that will be used by the clients to connect to the application server in order to establish the callback connection. The host name must be configured so that when used from the interactive clients it resolves to the application server on the configured port.

6. If using a load balancer, enter the required **Load Balancer Name**. If no load balancer name is entered, the host name will be used to establish the callback connection.

7. Enter the required **Inbound Port** and **Outbound Port** for the selected callback protocol. If using gRPC, only the inbound port value is configurable. If using WCF, both values are configurable.

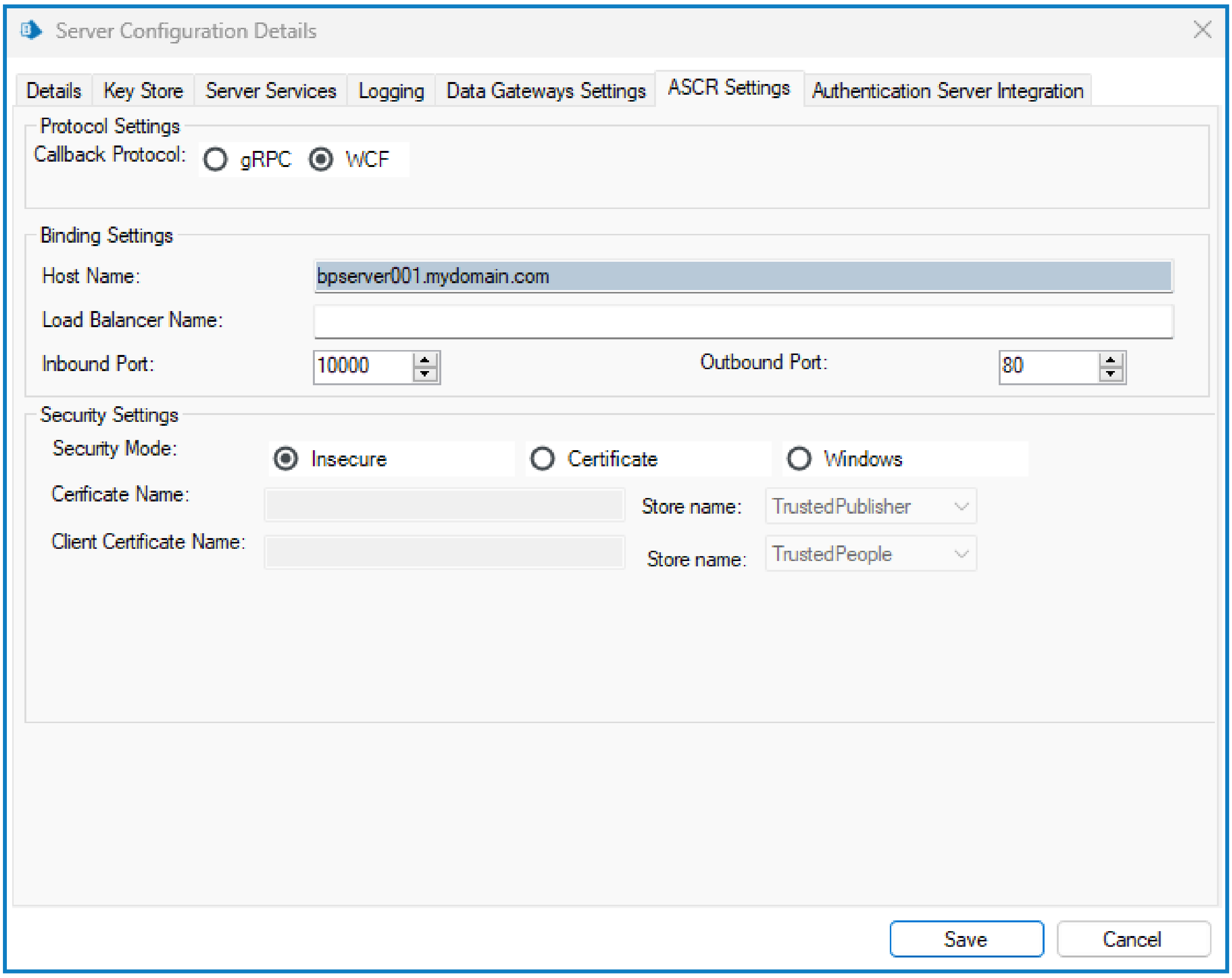
   > The configured ports will need to be opened on all Blue Prism application servers and interactive clients.
   >
   > It is generally assumed that outbound ports are not blocked by firewall settings in most environments. If outbound ports are blocked in your environment, please ensure that port 10000 (or the specified port for ASCR communication if the default is not used) is not blocked under your firewall rules. Outbound ports from the interactive client and inbound ports on the application server should be open on the configured port (default 10000).

Callback protocol	Machine	Inbound (listening) port	Outbound port
gRPC	Application server Interactive client	10000 (default) N/A	N/A High port range (49152 – 65535)
WCF	Application server Interactive client	10000 (default) 80 (default)	High port range (49152 – 65535) High port range (49152 – 65535)

> When using WCF, the command below must be run on the user's machine on which the interactive client is installed. This is because the incoming port must be bound to the user on the client machine if that user is not a local admin. A firewall inbound exception may be required on the client machine for the specified port, 80 in this example.

```
netsh http add urlacl url=http://+:80/bpinstruct  user="domain\user"
```

Where the application server outbound port 80 acts as the inbound port 80 for the interactive client.



Server Configuration Details

Protocol Settings

Callback Protocol: ○ gRPC ● WCF

Binding Settings

Host Name: bpserver001.mydomain.com

Load Balancer Name:

Inbound Port: 10000

Outbound Port: 80

Security Settings

Security Mode: ● Insecure ○ Certificate ○ Windows

Cerficate Name:

Store name: TrustedPublisher

Client Certificate Name:

Store name: TrustedPeople

8. Under Security Settings, select the **Security Mode** that you want to apply to the duplex channel from the following options:

Certificate	Use a Secure Socket Layer (SSL) certificate.
Windows	Windows integrated authentication and security. This option is available for the WCF callback protocol only.
Insecure	The callback protocol will not be secured.

9. If you select the Certificate security mode, the following certificate options are enabled and must be completed:

Certificate name	This requires a certificate configured for the host name endpoint. See Certificate requirements for details. The certificate name is the *Subject Name*, however, for cases where multiple similar subject names exist, the *Full Distinguished* subject name can be used.
Store name	Select the name of the store from which the application server certificate will be retrieved.
Client certificate name	This requires a certificate configured for the host name endpoint. The client certificate needs to be configured for the same end point on the server. See Certificate requirements for details. The certificate name is the *Subject Name*, however, for cases where multiple similar subject names exist, the *Full Distinguished* subject name can be used.
Store name	Select the name of the store from which the interactive client certificate will be retrieved.

10. Click **Save** to save the changes and apply the security settings.

ASCR configuration via command line

The ASCR settings can also be configured via AutomateC using the following commands:

```
AutomateC/ascrconfig <servername> <conntype> [1 - grpc | 2 - wcf] <hostname> <port>
<outbound port (wcf only)> <connectionmode> [1 - certificate | 2 - windows (wcf only)
| 3 - insecure] <certificatename> <clientcertificatename> <ascrservercertstore>
<ascrclientcertstore> [/loadbalancername <string>]
```

The certificate options are only required when `<connectionmode>` specifies certificates.

The following table lists relevant commands and possible values:

Commands	Values
`<conntype>`	• 1 – grpc • 2 – wcf
`<servername>`	The name of the server configuration in BPServer.exe. By default this is *Default*.
`<connectionmode>`	• 1 – certificate • 2 – windows • 3 – insecure
`<port> <outbound port (wcf only)>`	The value of the outbound port if using WCF. The default value is 80.
`/loadbalancername <string>`	The name of the load balancer if used. This command is optional.

> For further information about these and other commands, see the command line help by entering `/help` from an AutomateC command line.

Certificate requirements

> The Certificate security mode encrypts all data exchanged between client and server. Given the ASCR channel utilizes WCF messaging, the main purpose of certificate security is to encrypt the runtime resource change data events rather than authenticate identity.

If you have chosen to use the Certificate security mode, you will need a server and a client certificate, both of which must exist in the specified certificate store on the application server. The client certificate will be provided on-demand to an establishing client connection.

The certificate or certificate pair must meet the following requirements:

gRPC only

- Use an RSA Cryptographic Service Provider.
- Both certificates must include an exportable private key

WCF and gRPC

- Certificate DNS must align to the configured hostname.
- Include a private key.
- Client certificate must include an exportable private key.
- If different, the server and the client certificate must be signed against the same authority.

Direct database connection to runtime resources

To prevent potential performance issues caused by high numbers of resources, if an interactive client connects directly to the SQL server rather than via an application server, the following controls are applied during login:

- If fewer than 200 resources are detected, the connections are made and no warning messages display.
- If between 200 and 800 resources are detected, a message displays prompting the user to choose whether or not to connect to the resources. If the user chooses not to connect, the connections to the resources are disabled.

  > If the user chooses not to connect to the resources, the status of the resources can be still be viewed in Control Room, but they cannot be instructed by the interactive client in use.

- If more than 800 resources are detected, the automatic connection is disabled and a warning displays notifying you that the connection has not been made.

In the Blue Prism interactive client Control Room, the **Toggle Connections** menu option can be used to toggle the direct connection to the runtime resources on and off, as required.

ASCR troubleshooting and logging

This section offers guidance on the troubleshooting and logging of potential issues that users may encounter when using ASCR.

ASCR

When instructing a runtime resource from Control Room, the interactive client checks if the ASCR channel is currently running and attempts to reconnect if necessary. If the channel is not running, then a message displays informing the user that the channel is down, and offers troubleshooting advice. It may, however, be necessary to enable and view the relevant log file.

ASCR logging

For details on nLogging, logging levels, and how to enable logging, see Troubleshooting – Logging.

To include log messages from ASCR connections in the log files, depending on the log level that you require, you will need to add the following line to the **Automate.NLog.config** file on the client VM/PC and the **Server.NLog.config** file on the application server:

```
<logger name="BluePrism.ClientServerResources.*" minlevel="Trace" writeTo="app-logfile" />
```

or

```
<logger name="BluePrism.ClientServerResources.*" minlevel="Debug" writeTo="app-logfile" />
```

gRPC-related logs from ASCR connections are also displayed in logs generated by nLogs to allow users to assess error messages from gRPC connections in Production environments.

ASCR connections and load balancers

This information applies to Blue Prism 7.0 and 7.1 only.

When load balancing connections from interactive clients to application servers, if an application server unexpectedly goes offline, the ASCR callback channels do not fail over to another application server. Instead, the ASCR callback channels continue to try and connect to the currently unavailable application server. This happens because the callback communication channels used by ASCR are not load balanced along with the main data connection for the client.

If an application server unexpectedly terminates or becomes unresponsive, restart the interactive client. This will establish a connection with a functional application server, to which ASCR callback communication channels can then be established.

gRPC and WCF channels

If the interactive client fails to make a successful connection with the host , an error message displays, informing the user that the interactive client has failed to connect to all addresses. The connection from the interactive client to the host may fail for the following reasons:

- **Unresolvable ASCR configuration** – This is a result of incorrect, or no configuration, such as the host name is unresolvable, or the defined port is blocked on the Blue Prism interactive client or application server.

If the host name on the application server is correct and can be resolved via a nslookup <APPSERVERNAME> command from the machine where the interactive client is installed, but the "failed to connect" error message persists:

1. Close the Blue Prism interactive client.
2. Create a batch file on the machine where the Blue Prism interactive client is installed with the following contents:

   ```
   set GRPC_DNS_RESOLVER=native
   start ""
   "C:\Program Files\Blue Prism Limited\Blue Prism Automate\Automate.exe"
   ```

3. Run the batch file to start the interactive client.
4. If this doesn't fix the issue, set the ASCR host name on the application server to the numeric IP address of the Blue Prism application server.

- **Application server or interactive client certificate does not meet requirements** – See ASCR server configuration for details of certificate requirements and configuration.