

Esta guía detalla los pasos necesarios para la instalación y configuración de Aranda Virtual Support (AVS) en un entorno local. AVS es una aplicación de soporte remoto desarrollada por Aranda Software que permite tomar control remoto y transferir archivos en tiempo real y de forma segura a estaciones de trabajo.

¿Cuál es nuestra documentación?

- Guía de Inicio AVS
- Manual de Usuario Gestión AVS
- <u>Manual del Agente AVS</u>
- Manual Instalación On premises

Pre requisitos

Pre requisitos

Requisitos del sistema

Los siguientes requerimientos se definen para la implementación de Aranda Virtual Support en una instalación en entorno local.

	Servidor de Aplicaciones Web / Servicios
Dedicación	Uso dedicado para AVS (No compartir su uso con otras aplicaciones)
Almacenamiento	 - Espacio Requerido: Mínimo 64GB - Tipo de Unidad: Unidad de Estado Sólido(SSD) - Particiones: Se recomienda partición dedicada para la instalación del sitio. Se recomienda una partición dedicada para la base de datos (archivos MDF y LDF)(*) * En el caso de instalación de la solución en el mismo servidor donde reside la base de datos.
Procesamiento	4 CPU / 8 vCPU 2.1 GHz o superior.
Conectividad	Tarjeta de red Gigabit Ethernet (1GBps o superior)
Base de datos	 Versiones: SQL Server 2019, SQL Server 2022 Ediciones: Estandar (para Entornos de Pruebas), Enterprise (para Entornos Productivos) y Express (sólo para Pruebas de Concepto). Licenciamiento: Se recomienda licenciar la base de datos por Core. Collation: SQL_Latin1_General_CP1_CI_AI Permisos: Usuario para la creación de la base de datos (DBTools): Miembro del rol fijo <i>db_owner</i>. Usuario de servicio de la base de datos: Miembro del rol fijo <i>db_datareadery</i> <i>db_datawriter</i>. Permisos de ejecución sobre el esquema dbo
Sistema Operativo	Versión : Windows Server 2019, Windows Server 2022. Edición: Estándar o Superior. Cuenta de Instalación: Se requiere credenciales de administrador local y/o de dominio para la instalación.
Protocolos	- La aplicación funciona solo con HTTPS. - Se debe habilitar Websockets en toda la red. Lo requerido para que WebRTC opere correctamente.
Puertos de entrada	- Se debe habilitar el puerto para hace uso de HTTPS (por ejemplo 443). - Así mismo el puerto configurado para el turn y stun server.
Servicio de actualización	El servidor del Worker debe configurarse para poder alcanzar el sitio https://download.arandasoft.com/updates y descargar archivos.

Requerimientos adicionales

- Internet Information Services (IIS) 10.0 o superior.
- Roles
- File and Storage Services

* Storage Services * Web Server

* Common HTTP Features

- * Default Document
- * Directory Browsing * HTTP Errors

- * Static Content * Health and Diagnostics
- * HTTP Logging * Performance
- * Static Content
- * Security
- * Request Filtering * Application Development



▷ **Nota:** Antes de iniciar la instalación de Aranda Virtual Support es necesario crear el esquema de base de datos a través del módulo **Aranda Database Tools v9**.

Consulte el Manual de usuario de Aranda Database Tools V9

Servicio de licenciamiento

Aranda Virtual Support (AVS) utiliza el servicio común de licenciamiento de Aranda para autorizar el ingreso a usuarios al sitio web de AVS y controlar las licencias compradas, entre otras operaciones. Este es un servicio de Windows que normalmente es creado de manera automática por el instalador del producto. Una vez el usuario cargue desde el sitio web sus licencias compradas, el servicio común de licenciamiento debe permanecer en la misma máquina, de otra manera las licencias cargadas se perderán. Si su servidor de aplicaciones se encuentra ubicado en una máquina virtual se recomienda instalar el servicio común de licenciamiento en una máquina física, ya que al reiniciar máquinas virtuales existe una alta probabilidad de que la marca de hardware cambie y el servicio asuma incorrectamente que fue trasladado. Consulte con el proveedor para más detalles sobre el despliegue del servidor.

Instalación de AVS

Instalación de AVS On Premise

El instalador **AVS.Server.Installer** instala cinco sitios web (agentavs, arc/notification, arc/Recording, avs, notificationavs).



Y cinco servicios Windows (Aranda License Windows Service, Aranda Scheduler Windows Service, Aranda Worker Windows Service, Aranda AVS Turn Server y Aranda AVS Stun Server).



1. Haga doble clic sobre el archivo del instalador y visualizará la pantalla de bienvenida. Confirme la instalación haciendo clic en el botón **Siguiente**.

Rranda Virtual Support Server - InstallShield Wizard					
2	Welcome to the InstallShield Wizard for Aranda Virtual Support Server				
	The InstallShield(R) Wizard will install Aranda Virtual Support Server on your computer. To continue, dick Next.				
WARNING: This program is protected by copyright law and international treaties.					
	< Back Next > Cancel				

2. En la ventana Información del cliente, ingrese el nombre de usuario, la organización y haga clic en Siguiente.

🕼 Aranda Virtual Support Server - InstallShield Wizard	×
Customer Information	4.
Please enter your information.	
User Name:	
Organization:	

InstallShield			
	< Back	Next >	Cancel

3. En la ventana **Tipo de instalación** podrá configurar las siguientes opciones:

- Completa: Se instalarán todos los sitios y servicios en las rutas por defecto.
- Personalizada: Podrá seleccionar los sitios o servicios que desea instalar.

▷ Nota: De forma predeterminada, seleccione el tipo de instalación Completa. En el caso de establecer separación de las capas de la solución (Web, Aplicación) en servidores independientes, seleccione la opción Personalizada.

△ Importante: Si va a realizar una instalación personalizada, no modifique la ruta de instalación.



🖟 Aranda Virtual Support Server - InstallShield Wizard	×
Custom Setup Select the program features you want installed.	と
Click on an icon in the list below to change how a feature is in	stalled.
ARC Turn Server Web ARC Notification ARC Recording AVS Services Common License Stun/Turn WebRTC	Feature Description This feature requires 72MB on your hard drive.
Install to: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn (Server
C. Programmies (2007 pranta pranta Renote Control (1011)	Change
InstallShield	
Help Space < Back	Next > Cancel

4. Configurado el tipo de instalación, en la ventana **Preparando para instalar el programa**, haga clic en **Siguiente** y luego en el botón **Instalar**.

🕼 Aranda Virtual Support Server - InstallShield V	Nizard X
Ready to Install the Program The wizard is ready to begin installation.	と
Click Install to begin the installation.	
If you want to review or change any of your inst exit the wizard.	tallation settings, click Back. Click Cancel to
InstallShield	
< B	lack Install Cancel

5. Al terminar el proceso de instalación, haga clic en el botón Finalizar.

Configuración conexión con base de datos

Una vez finalice la instalación de **Aranda Virtual Support**, proceda a configurar las cadenas de conexión hacia la base de datos de los sitios y servicios.

Configurar sitios

Para configurar los sitios web actualice el valor de la cadena de conexión, en la línea 6 dentro de los archivos appsettings.json de cada sitio; las rutas por defecto son:



Ejemplo de cómo debe quedar la cadena de conexión en el appsettings.json



Tener presente que se deben incluir las propiedades Encrypt y TrustServerCertificate y el valor se asigna de acuerdo a las reglas de negocio del cliente. <u>Ver documentación de Microsoft</u>

Configurar servicios comunes

Para configurar los servicios Comunes y de Licenciamiento, se realiza a través del módulo**Aranda Database Tools v9**. Para ello:

1. Ejecute el módulo y haga clic en la pestaña Connection String.

📰 Aranda Database tools						-		×
Packages Connection String	Services							
SqlServer 🗸	Connection N	lame	Database					
Server Name	User Name		*****	Encrypt	Trust server certificate	Cancel Test	Save	:
Name			Provider		Server	Database		



2. Complete los datos solicitados.

- Seleccione el motor de base de datos (SQL Server).
- Asigne un nombre para identificar la conexión.
- Registre los datos de conexión (nombre de la base de datos, nombre del servidor o dirección IP, y si se requiere usuario y contraseña).
- En caso que el puerto de base de datos sea distinto al puerto establecido por defecto (1433 para SQL Server), se debe escribir el servidor como servername:port (ej. ARANDADBSERVER:5555)

• De forma predeterminada, se debe marcar la opción "Encrypt" para asegurar que la conexión entre la solución y la base de datos está encriptada.

🗮 Aranda Database tools					_ = ×
Packages Connection String	Services				
SqlServer 👻	ArandaConn	AIS_001_MARKS			
20.231.124.106	avs, administration	********	Encrypt Trust server of	ertificate Cancel	Test Save
Name		Provider	Server	D	atabase
Allow House					Apply Update
New item					Apply Opdate

3. Haga clic en el botón **Test** para comprobar la conexión.

Packages Connection String Service	5						
SqlServer	aConn	art, one search]				
20.251.124.188	Interstation	*****	Encrypt	Trust server certificate	Cancel Test	Sav	e
Name		Provider		Server	Database		
New Per		Test connection Connection success OK		X	Anti-	104	hie

4. Para finalizar haga clic en el botón **Save** para guardar la conexión.

🗒 Aranda Database tools				_ = ×
Packages Connection Strip	ng Services			
SqlServer	 ArandaConn 	AV5,01Y,MAWUEL		
20,231,134,186	ave_administ	utor	Encrypt Trust server certificate	New Test Save
Name		Provider	Server	Database
ArandaCor	nn	SqlServer	20,211,124,186	AND DRY MARKED.



5. Para aplicar las cadenas de conexión a los servicios instalados, seleccione la conexión creada previamente y haga clic en el botón **Apply.**



6. Se habilita una ventana con el listado de aplicaciones y servicios disponibles en el servidor.

🗮 Arand	a Database tools	-		×
Packages	Connection String Services			
SqlServe	🗒 Config Files 🛛 🗙 🗙			
28.231.1	Web Applications ✓ Windows Services		Sav	e
	C:\Program Files (x86)\Aranda\Aranda License\Aranda.License.Windows.Service.exe.config			Τ
	Cancel Apply			
	Аррђ		Upda	te

7. Seleccione los servicios correspondientes y haga clic en el botón **Apply**, si desea encriptar la conexión marque la casilla **Encrypt** ubicada en la esquina inferior izquierda. Se podrá visualizar un mensaje de alerta porque la encriptación no está soportada para archivos JSON.

8. Para finalizar haga clic en la pestaña **Services** e inicie todos los servicios.

🗒 Aranda Database tools			-		×	
Packages Connection String Services						
DisplayName ServiceName State						
Aranda License Windows Service	ArandaLicenseWindowsService	Stopped				
Aranda Scheduler Windows Service	ArandaSchedulerWindowsService	Stopped				



△ Importante Cuando se realicen cambios a las cadenas de conexión de los sitios, se debe reiniciar o reciclar el grupo de aplicaciones asociado al sitio para que el cambio se aplique inmediatamente.



9. Establecida la conexión, podrá acceder al sitio web de AVS donde podrá iniciar con la configuración de Aranda Virtual Support a través de la siguiente URL: *https://dns_servidor/avs/.*

← C ⊕ https://dns-dominio/avs/	3 🕸 🤇
Aranda	Aranda Virtual Support
	Enter the information to access
	Authentication type
	User
	Enter username
	Password
	Enter password 📀
	Sign in
Copyright © Aranda Software.	
Arondo VIRTUAL SUPPORT Version 0.0.0.0	

Licenciamiento de AVS

Todos los productos de Aranda Software requieren una licencia para su funcionamiento, por tal razón, la primera vez que ingrese al sitio web de Aranda Virtual Support (AVS), seleccione la opción Licencias del menú principal en donde podrá agregar nuevas licencias y visualizar el listado de licencias existentes agrupadas con los siguientes datos:

Columna	Descripción
Nombre	Es el nombre del producto de Aranda asignado a la licencia.
Тіро	Tipo de licencia.
Usuarios	Número de usuarios concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Sesiones de soporte	Número de sesiones de soporte concurrentes (Cantidad usada/cantidad total de licencias).
Dispositivos	Número de estaciones de trabajo concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Empresa	Empresa dueña de la licencia.
Fecha de activación	Fecha en la que son activadas las licencias.
Fecha de expiración	Fecha de caducidad de las licencias.

En la ventana Licenciamiento haga clic en NUEVA LICENCIA.



En la ventana emergente seleccione la opción **Descargar**, que permite la descarga del archivo MachineKey.amk, el cual debe ser enviado al área encargada en Aranda Software (Preventa y Proyectos) para la generación del archivo .lic (archivo de licenciamiento).

	A
nt to do with MachineKey.amk?	
Save as \sim	
In order to activate the license, please attac	h the
The extension (.lic) that you received by e-m	11.
~	
(†)	
<u>O files</u>	
Select files to attach	

Una vez recibido el archivo .lic debe cargarlo al servidor, haga clic en el botón Seleccione archivos a adjuntar y luego en Guardar (ícono en forma de disquete). Al cargar la licencia es generada la alerta correspondiente.

SETTINGS	>	Licensing You can then manage licenses and/or associate them to specific devices.			8	Attach file for license	>
		Q Search	NA	Name		In order to activate the license, please attach the	
neral configuration		□ Name ∨ Type ∨ Users Support sessions		VALID		hie extension (.lic) that you received by e-mail.	
Users			How to	get the file (.lic)		Â	
User groups				Download		<u>O files</u>	
Licenses		×	l 🐻	Click here to download the file (.amk)		Select files to attach	
- → ✓ ↑ • • • • • • • • • • • • • • • • • •	eta	Laur > AVS-A C Buscar en AVS-AZURE P E C Fecha de modificación Tipo To	R.	Verify In the next few hours you will receive the file (.lic) in your e- mail.			
1 License_31108.	lic	13/11/2024 2:17 p. m. License					
Nombre	de ar	rchivo: License_31108.lic v License (*.lic) v					

Para conocer en detalle la licencia, en la ventana Licenciamiento, seleccione un registro del listado de licencias disponibles y en la ventana que se habilita podrá visualizar la vigencia de la licencia y el número de licencias que se han usado por usuarios, sesiones de soporte y dispositivos concurrentes (Cantidad de licencias usadas/cantidad total de licencias).



Para eliminar una licencia, en la ventana Licenciamiento seleccione el registro de la licencia que desea eliminar y haga clic en el botón Eliminar, se confirmará que la licencia ha sido eliminada satisfactoriamente.

🗱 🗇 Aranda Virtua	l Sup	oport												AA
	>	Licensing You can the	en mono	e licens	es and/or ass	ociate them to	o specific devices.							
		Q. Sea									NEW LICENCE	🗊 Delete	Y Clear filters	Column options 🗸
General configuration ୟସ୍ଟିସ୍ଥ Users			lome 🕓		Туре \vee	Users	Support session	is Devi	ices Comp	any 🗸	Activation	date 💛	Expiration d	late 💛
🛞 User groups														
Elicenses														
					2	Licen	ses or the license	e has been succ	essfully remo	ved.	×			
														0 de 0 records

Configuraciones posteriores

Configuración de Infraestructura

Después de instalar los sitios y servicios de Aranda Virtual Support (AVS), es necesario realizar algunas configuraciones desde el sitio web de AVS para garantizar el correcto funcionamiento de la aplicación durante los procesos de control remoto y transferencia de archivos. Por lo tanto, se recomienda seguir los siguientes pasos:

1. Ingresar al sitio web

Ingrese al sitio web de AVS con un usuario que tenga el rol de Administrador General o Infraestructura. Estos roles tienen los permisos necesarios para gestionar las opciones de Servidores Turn externos, Servidor Turn local y Almacenamiento. Es importante tener en cuenta que estas opciones están disponibles únicamente en instalaciones On Premise.

000 000 000	🖨 Aranda Virtu	ual S	Support					AA
Ø	SETTINGS	0	External Turr Configure the Tur	servers n servers to establish the conr	nection between the specialist and th	e workstation.		
8	Support Groups		-					New Delete
	Agent profiles		U	Name		User	Un	
52	Support sessions							
R.	Auditory							
	External Turn servers							
	Local Turn Server							
	Storage							
Gen	eral configuration							
898.	Users							
3	User groups							
۲	Licenses							
	Directory services							
0	External authentication							Showing – to – of 0 records

2. Servidores Turn Externos

La funcionalidad de transferencia de archivos de AVS utiliza un protocolo P2P basado en WebRTC. Cuando dos dispositivos no pueden establecer una conexión directa entre sí, se necesita un servidor Turn para facilitar la comunicación.

Para agregar un servidor Turn externo en la ventana de Servidores Turn Externos, siga estos pasos:

A. Haga clic en la opción Nuevo.

B. Complete los campos solicitados de acuerdo a la siguiente tabla:

Campo	Descripción
Nombre	Nombre que se le desea asignar a la configuración, entre 6 y 50 caracteres.
URL	Corresponde al sitio del servidor STUN/TURN, por ejemplo: turn: <server_public_ip>:puerto o stun:<server_public_ip>:puerto .</server_public_ip></server_public_ip>
Usuario	Nombre del usuario autorizado para conectar al servidor STUN/TURN.
Contraseña	Contraseña asociada al usuario que permite la conexión con el servidor STUN/TURN.

C. Finalice haciendo clic en el botón **Guardar**.

▷ Nota: Esta configuración es requerida para la transferencia de archivos cuando el agente especialista y el agente de la estación de trabajo no están en la misma red, por lo tanto, se debe permitir la salida a Internet de ambos dispositivos por el puerto configurado.



El usuario puede registrar la cantidad de servidores Turn externos que considere necesarios (máximo 10) para tener una buena comunicación entre los dispositivos del especialista y la estación de trabajo a través de la consola de AVS.

Para eliminar un servidor Turn externo, en la ventana Servidores Turn Externos seleccione el o los servidores a eliminar y haga clic en el botón Eliminar. Se confirmará que el o los servidores han sido eliminados exitosamente.



Se pueden utilizar STUN/TURN WebRTC públicos, realizando una búsqueda en la web "STUN server list" se podrán listar los diferentes servidores STUN/TURN públicos disponibles. Al configurar servidores públicos en las estaciones de trabajo y en los equipos especialistas deben permitir la salida hacia los sitios de los servidores que se configuren. También es posible configurar el servidor STUN/TURN provisto en el instalador <u>realizando los ajustes en el servicio</u> <u>Aranda Turn Stun WebRTC Server Windows Service</u>. Además, se pueden utilizar STUN/TURN públicos junto con servidores propios instalados, como se mencionó anteriormente.

3. Servidor Turn Local

Para establecer la comunicación de toma de control remoto entre el agente especialista y el agente de la estación de trabajo, utilice un servidor Turn local que puede retransmitir el tráfico de red.

Para agregar un servidor Turn local, siga estos pasos:

A. Haga clic en la opción Servidor Turn local del menú principal.

B. Complete el campo Host con la ruta de acceso al servidor local, que puede ser la IP del servidor o el DNS. El campo Port esta configurado por defecto con el valor 8081 y el SSL inactivo, si se cambia el puerto o se activa el SSL se deben <u>realizar los ajustes en el servicio Aranda AVS Turn Server</u> instalado en el servidor.

C. Finalice haciendo clic en el botón Guardar

🗱 🖨 Aranda Virtual Support		AA
Support Groups Agent profiles Support sessions Support sessions Support sessions Additory External Turn servers Contran Server Storage Ceneral configuration Storage Users Users User groups Licenses Directory services Directory services External turn server	Turn Server Local Define fileIds for configuration Host Enter the provider URL. Write Porto Enter the port associated with the server @ddl Boble SSL	

4. Almacenamiento

Esta configuración es necesaria para almacenar las grabaciones de la prestación del servicio de control remoto y los instaladores del agente para las estaciones de trabajo. Los archivos generados se envían a un proveedor de almacenamiento. El proveedor puede ser de tres tipos: local, remoto o Blob storage.

Para configurar el proveedor de almacenamiento, siga estos pasos:

A. Haga clic en la opción Almacenamiento del menú principal.

B. Complete el campo o los campos solicitados dependiendo del tipo de almacenamiento seleccionado.

C. Finalice haciendo clic en el botón Guardar

🗱 🗇 Aranda Virtual S	Support		AA
SETTINGS Support Groups Agent profiles Support sessions Auditory External Turn servers Local Turn Server Storage General configuration RR Users Directory services Directory services External	Select the option for the creation of the storage storage.	 Configure file storage Betty pe of supplier: Configure the Blob Storage connection path Configure the Blob Storage connection path *Add the connection string The the stable of the enclosed blob enclos	

\triangleright Notas:

- Para que las grabaciones se almacenen de forma correcta, el servidor donde está instalado el sitio d e avs y arc/recording debe contar con acceso al proveedor configurado. En caso de utilizar el proveedor tipo local, la ruta debe existir en el servidor y tener los permisos correspondientes.
- Para que los instaladores se almacenen de forma correcta, el servidor donde estén instalados los servicios Comunes (Worker) debe contar con acceso al proveedor configurado. En caso de utilizar el proveedor tipo local, la ruta debe existir en el servidor y tener los permisos correspondientes.
- Si el **Worker** y el sitio del **agentavs** están instalados en servidores independientes, se debe garantizar que ambos puedan acceder al almacenamiento configurado, para que la actualización de agentes se realice de forma correcta.
- Si, posterior a la configuración, se realizan cambios en el proveedor de almacenamiento, es necesario mover la información contenida en el proveedor anterior al actual. Si no se realiza esta acción, las actualizaciones de los agentes no se realizarán de forma correcta y no se podrá acceder a las grabaciones en las auditorías.

Configuración manual de servicios

Configuración del Turn Server

← Servidor Turn Local

Después de instalar el servicio Aranda AVS Turn Server, no es necesario realizar ningún ajuste para su funcionamiento. Sin embargo, se pueden realizar parametrizaciones según las necesidades específicas, como cambiar el puerto de conexión (8081 por defecto) y habilitar el SSL (deshabilitado por defecto). Si necesita realizar estas parametrizaciones, siga los siguientes pasos:

1. Validación del Archivo appsettings.json

Antes de realizar cambios, verifique el archivo **appsettings.json** ubicado en la ruta de instalación del servicio (por defecto: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) para asegurarse de que el puerto esté configurado por defecto en 8081. Si no es necesario modificar el puerto, no es necesario realizar más ajustes.

Adicionalmente valide que el puerto 8081 esté habilitado en las reglas del firewall local para garantizar el flujo correcto del tráfico. En este archivo, también puede encontrar la configuración para los certificados SSL, que por defecto se encuentra desactivada (IsSsI=false).

Turn Server			_		×
Share View					~ (
C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Se	rver ~	Ō			Q
Name ^	Date modified		Туре	Size	
Logs	11/15/2024 12:0	2 AM	File folder		
📓 appsettings.json	9/12/2024 8:57	M	JSON File		1 KE
Aranda.AVS.Turn.Common.dll	11/1/2024 11:52	AM	Application exten		24 KE
🚳 Aranda.AVS.Turn.Domain.dll	11/1/2024 11:53	AM	Application exten		21 KI
Aranda.AVS.Turn.Infrastructure.dll	11/1/2024 11:53	AM	Application exten		50 KI
🍸 Aranda.AVS.Turn.Service.deps.json	9/12/2024 8:57	MA	JSON File		28 K
Aranda.AVS.Turn.Service.dll	11/1/2024 11:53	AM	Application exten		23 K
💽 Aranda.AVS.Turn.Service.exe	11/1/2024 11:53	AM	Application	1	60 K
🎽 Aranda.AVS.Turn.Service.runtimeconfig.json	9/12/2024 8:57	MA	JSON File		1 K
FluentValidation.dll	9/12/2024 8:57	MA	Application exten	4	458 K
Microsoft.Extensions.Configuration.dll	9/12/2024 8:57	MA	Application exten		39 K
Microsoft.Extensions.Configuration.EnvironmentVariables.dll	9/12/2024 8:57 4	MA	Application exten		19 K
Microsoft.Extensions.Configuration.UserSecrets.dll	9/12/2024 8:57	MA	Application exten		25 K
Microsoft.Extensions.Hosting.dll	9/12/2024 8:57	MA	Application exten		55 K
Microsoft.Extensions.Hosting.WindowsServices.dll	9/12/2024 8:57 4	MA	Application exten		24 K
Newtonsoft.Json.dll	9/12/2024 8:57	MA	Application exten	6	596 K
🝸 nlog.config	9/12/2024 8:57	MA	CONFIG File		1 K
NLog.dll	9/12/2024 8:57	MA	Application exten	8	323 K
NLog.Extensions.Logging.dll	9/12/2024 8:57	MA	Application exten		61 K
NLog.Web.AspNetCore.dll	9/12/2024 8:57	MA	Application exten	1	103 K
System.ServiceProcess.ServiceController.dll	9/12/2024 8:57	MA	Application exten		61 K

Configuración por defecto de appsettings.json:



2. Cambio de Configuración del Puerto

Edite el archivo *appsettings.json* y configure el puerto deseado reemplazando <puerto> por el número de puerto deseado.

"Turr	Configuration": {
"Ce	ortificateParam"."
"Ca	artificatePath"."
"Cc	rtificatoSubicot"."
UE "Iot	Dell's false
IS: "D-	psi:iuise,

"SSLProtocols": "TIs12"

3. Configuración de conexión segura SSL

Edite el archivo *appsettings.json*, cambie "IsSsl" a true. Para agregar el certificado SSL hay dos alternativas:

3.1. Adquirir o generar un certificado PFX, el cual deberá ser ubicado dentro de la carpeta **Resources** (la carpeta se debe crear si no existe) en la ruta de instalación del servicio.

Res	ources						_	\times
	Share	View						~ ?
	« Aranda	a → Aranda Remote	Control > Turn Server > Resources	~	Ū	Search Reso	urces	Q
Na	ame	^	Date modified	Туре		Size		
5	Cert_Nar	ne.pfx	11/15/2024 12:10 AM	Persona	l Infori	mati	3 KB	

El nombre del archivo se registra en la opción **CertificatePath** y la clave codificada en base 64 de generación del certificado se debe registrar en **CertificateParam**, ambas opciones disponibles en el archivo *appsettings.json*.

TurnConfiguration": {			
"CertificateParam": " <clave-base64>",</clave-base64>			
"CertificatePath": " <nombre-archivo.pfx>",</nombre-archivo.pfx>			
"CertificateSubject": "",			
"IsSsI": true,			
"Port": 8081,			
"SSLProtocols": "TIs12"			
}			

3.2. Si tiene almacenado un certificado PFX en el depósito de certificados, puede configurarlo mediante el nombre del mismo en la opción **CertificateSubject** del archivo *appsettings.json*.

"TurnConfiguration": { "CertificateParam": "".	
"CertificateParam": "".	
"CertificatePath": "",	
"CertificateSubject": " <nombre-certificado>",</nombre-certificado>	
"IsSsI": true,	
"Port": 8081,	
"SSLProtocols": "TIs12"	
}	

4. Reinicio del Servicio

Reinicie el servicio del Turn Server (Aranda AVS Turn Server) para que los cambios en la configuración surtan efecto. El servicio ahora debería escuchar en el nuevo puerto configurado y habilitar el uso de certificado SSL.

5. Configuración del Firewall

Abra el puerto que se configuró en el paso 2 en las reglas de entrada del firewall local. Este paso es crucial para permitir el tráfico a través del nuevo puerto y asegurar que el Turn Server pueda recibir conexiones entrantes en el puerto configurado.

Parametrizar el puerto del Turn Server y el uso de SSL desde el servicio es un proceso fundamental para garantizar su correcto funcionamiento y adaptarlo a las necesidades específicas de cada cliente. Siguiendo estos pasos, puede asegurarse de que el Turn Server esté configurado correctamente y listo para manejar las conexiones según lo requerido.

<u>← Servidor Turn Local</u>

Configuración del Servidor STUN/TURN WebRTC

← Servidor TURN Externo

Después de instalar el servicio Aranda Turn Stun WebRTC Server, es necesario realizar la configuración para que este

pueda funcionar correctamente.

1. Validación del Archivo turn-server.toml

Antes de realizar cambios, verifique que el archivot**urn-server.toml** se encuentre ubicado en la ruta de instalación del servicio (por defecto: C:\Program Files (x86)\Aranda Aranda Remote Control\Stun Server).

```
turn-server.toml C:\turn-server.toml
     [turn]
     realm = "localhost"
11
    [[turn.interfaces]]
    transport = "udp"
     bind = "127.0.0.1:3478"
23 # address and service listening port.
     external = "127.0.0.1:3478"
    [[turn.interfaces]]
    transport = "tcp"
    bind = "127.0.0.1:3478"
    external = "127.0.0.1:3478"
    [api]
     # This option specifies the http server binding address used to control
     # the turn server.
     # and sensitive information and dangerous operations can be obtained
    bind = "127.0.0.1:3000"
     # and sensitive information and dangerous operations can be obtained
     # through this service, please do not expose it directly to an unsafe
```

Para configurar el servicio STUN/TURN WebRTC, utilice el archivo turn-server.toml:

- Sección [turn]: Especifica el dominio donde se encuentra el servidor.
- Sección[[turn.interfaces]]: Indica las interfaces de escucha. Describe la interfaz a la que está vinculado el servidor STUN/TURN. Se pueden indicar varias interfaces.
- Sección [turn.interfaces.transport]: Define el tipo de transporte de la interfaz, que puede ser udp o tcp.
- Sección [turn.interfaces.bind]: Dirección IP y puerto de vinculación del socket interno.
- Sección [turn.interfaces.external]: Se usa para enlazar a la dirección de su NIC local. Por ejemplo, si tiene dos

NIC, A y B, en su servidor, y la dirección IP de la NIC A es 192.168.1.2 y la de la NIC B es 192.168.1.3, si se enlaza a la NIC A, debe enlazar a la dirección 192.168.1.2. Enlazar a 0.0.0.0 significa que escucha en todas las interfaces al mismo tiempo. La palabra external significa que su tarjeta de red para el cliente pueda "ver" la dirección IP. Continuando con el ejemplo anterior, si su tarjeta de red A se comunica con el exterior, los otros clientes verán su dirección LAN (es decir, 192.168.1.2). Sin embargo, en la realidad, la topología de red donde está desplegado el servidor podría tener otra IP pública, como 1.1.1.1, que es la dirección IP vista por los demás clientes. La razón por la que se necesitan bind y external es que, para el protocolo STUN, el servidor necesita informar su propia dirección IP externa, permitiendo así que el cliente STUN se conecte a la dirección especificada mediante la IP informada por el servidor.

- Sección [api.bind]: Escucha de la API para consultas, por ejemplo: http://127.0.0.1:3000/info.
- Sección [log.level]: Nivel de registro (log). Valores válidos: error, warn, info, debug, trace.
- Sección [auth]: Par de usuario y contraseña para acceder al servidor.

2. Inicio del Servicio

Inicie el servicio del STUN Server (Aranda Turn Stun WebRTC Server) para que los cambios en la configuración surtan

efecto.

3. Configuración del Firewall

Abra el puerto o los puertos configurados en el paso 1 en las reglas de entrada del firewall local y en los controladores de red presentes en la infraestructura del cliente, para los protocolos TCP y UDP. Este paso es esencial para permitir el tráfico a través del nuevo puerto y asegurar que el servidor STUN pueda recibir conexiones entrantes en el puerto configurado.

En las estaciones de trabajo (Agente AVS) y en los equipos especialistas (Agente especialista), deben permitir la salida por los puertos que se configuren.

Adicionalmente, si requiere que opere como TURN WebRTC, debe abrir el rango de puertos 49152-65535 para el protocolo UDP.

Ejemplo de configuración servicio STUN/TURN y escenarios

← Servidor TURN Externo

Ejemplo de configuración servicio STUN/TURN y Escenarios

← Servidor TURN Externo

Para que el servidor funcione tanto para dispositivos dentro como fuera de la red siga los siguientes pasos:

1. Configurar el realm

Cambie el valor de realm al dominio público o dirección IP externa de su servidor. Esto es importante para autenticar correctamente las solicitudes externas.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:



2. Configurar bind

La sección bind asegura que el servidor STUN/TURN escuche en la IP privada para las conexiones dentro de la red local.

Si la dirección privada de su servidor es 192.168.1.25, configúrelo como:

bind = "192.168.1.25:3478"

Si requiere que el servicio STUN/TURN escuche en todas las interfaces al mismo tiempo, configúrelo como:

bind = "0.0.0.0:3478"

Estas configuraciones sólo son requeridas para [[turn.interfaces]].

3. Configurar external

La sección external es donde se define la IP pública del servidor para que los equipos externos puedan comunicarse correctamente con el servidor STUN/TURN.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:

external = "1.2.3.4:3478"

4. Autenticación

La sección [auth] está configurada con usuarios estáticos:

Esto permite conexiones autenticadas con las credenciales estáticas user1:test y user2:test. Asegúrese de usar credenciales más seguras si planea exponer este servicio a dispositivos externos.

Los demás secciones de pueden dejar por defecto.

Al realizar la parametrización en el archivo turn-server.toml, este deberá observarse de la siguiente forma:



Cada vez que realice una modificación al archivo turn-server.toml, reinicie el servicio Aranda Turn Stun WebRTC Server para que los cambios surtan efecto.

Escenarios

A continuación, se describen los siguientes escenarios y el resultado de acuerdo con la configuración del ejemplo.

Escenario	Especialista	Estado en Red	Agente AVS	Estado en Red	Resultado
1	Solo puede acceder al servidor TURN/STUN usando la IP pública	Externo	Solo puede acceder al servidor TURN/STUN usando la IP pública.	Externo	El Especialista y el Agente AVS pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
2	Solo puede acceder al servidor TURN/STUN usando la IP pública.	Externo	Puede acceder al servidor TURN/STUN usando la IP pública.	Interno	El Especialista y el Agente AVS pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
3	Puede acceder al servidor TURN/STUN usando la IP pública.	Interno	Puede acceder al servidor TURN/STUN usando la IP pública.	Interno	El Especialista y el Agente AVS pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
4	Solo puede acceder al servidor TURN/STUN usando la IP privada.	Interno	Solo puede acceder al servidor TURN/STUN usando la IP privada.	Interno	El Especialista y el Agente AVS pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP privada.
5	Solo puede acceder al servidor TURN/STUN usando la IP pública.	Externo	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido a la red interna (IP privada).	Interno	El Especialista y el Agente AVS no pueden establecer comunicación debido a un problema de conectividad entre redes (exterior e interior).
6	Solo puede acceder al servidor TURN/STUN usando la IP pública.	Externo	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido.	Externo	El Especialista y el Agente AVS no pueden establecer comunicación debido a un problema de conectividad entre redes.

▲ Nota:

- Para cubrir los escenarios 1, 2 y 3, configure en el<u>sitio web de AVS</u> el servidor Turn Externo de la siguiente manera:
 - Nombre: nombre de la configuración.
 - URL: turn.1.2.3.4:3478 (1.2.3.4 hace referencia a la IP pública del servidor).
 - U**suario:** user1.
 - Contraseña: test.

\triangle Notas:

• Para cubrir el escenario (4), configure en el sitio web de AVS el servidor Turn Externo de la siguiente

manera: Nombre: nombre de la configuración. URL: turn.192.168.1.25:3478 (192.168.1.25 hace referencia a la IP privada del servidor). Usuario: user1. Contraseña: test.

• Si en el archivo turn-server.toml se configuró 0.0.0.0 en el parámetro bind, se debe realizar la configuración en el sitio como se indicó anteriormente.

← Servidor TURN Externo

Despliegue

Diagrama de despliegue

1. Diagrama

En la siguiente figura se tiene el diagrama de despliegue:



2. Servidores

La instalación en servidores la componen los siguientes elementos:

Servicios Windows: Permiten la ejecución de tareas, agendas, entre otras funcionalidades en segundo plano.

- Aranda AVS Turn Server: Permite la conexión de las puntas en una sesión de control remoto. Requiere escuchar en el puerto 8081, aunque puede ser configurado. Utiliza el protocolo TCP configurable a usar SSL/TLS
- Aranda AVS Stun Server: Permite contar con un servidor stun/turn WebRTC para la funcionalidad de transferencia de archivos. Escucha como mínimo en el puerto 3478 por TCP y UDP. Para permitir relay pueden configurarse más puertos por TCP o UDP.
- Servicios de la common: Servicios comunes de aplicaciones de Aranda.

Aplicaciones Web: Permiten exponer por HTTPS aplicaciones web. Todos utilizan el puerto 443 con protocolo TCP. Es requerido habilitar HTTPS

- API/AVS: Ofrece las funcionalidades de la página principal del producto Virtual Support.
- API/Agentavs: Permite registrar y actualizar las estaciones de trabajo.
- Notificationavs: Permite el envío de mensajes entre los especialistas y las estaciones de trabajo. Utiliza protocolo WebSocket

Servidor de base de datos: Servidor SQLServer persistir datos estructurados

3. Usuarios

Administradores: Gestionan configuraciones del producto. Utilizan un explorador web.

Especialistas: Utilizan los servicios de soporte como control remoto, transferencia de archivos y chat

- Página web: Utilizan las funcionalidades de soporte
- Aranda.AVS.Viewer.Console: Visor que permite tomar control remoto en las estaciones de trabajo.
- Aranda.AVS.Specialist.Orchestrator: Servicio Windows que permite la funcionalidad de transferencia de archivos y enviar grabaciones de control remoto.

Estaciones de trabajo: Reciben la ayuda a través de las funcionalidades de soporte. Se tiene soporte para Windows y Mac OS

- Aranda.AVS.Workstation: Servicio de Windows que ofrece las funcionalidades principales
- Aranda.AVS.VNC.Application: Servicio de Windows que permite tomar control remoto.