AnyDesk en pocas palabras: ACL y Namespace

> Ver video aquí

Hola, hoy vamos a trabajar en los conceptos de ACL o lista de control de acceso, y de namespace o espacio de nombres.

La configuración de las ACL se encuentra en el cliente de AnyDesk, en la sección de seguridad de acceso, y en el portal de administración **my.anydesk.com** en la creación de clientes personalizados.

Pasemos al tema. Como sabes, todos los dispositivos que se conectan a la red de AnyDesk tienen un identificador. El que puedes ver inicialmente es un identificador numérico. Aquellos usuarios que tienen una licencia de pago pueden cambiar ese identificador por un alias, que es mucho más fácil de recordar. Esta configuración se puede realizar haciendo clic derecho sobre el identificador y seleccionando el alias, o en **my.anydesk**, en los detalles del cliente, editando el cliente respectivo.

El alias está compuesto por dos partes: una identificación que debe ser única dentro del namespace, que es la segunda parte. Este namespace puede personalizarse. Las empresas pueden adquirir un espacio de nombres privado y único, lo que les permite identificar sus dispositivos de acuerdo con su identidad corporativa y también facilita la gestión de grandes cantidades de dispositivos.

Ahora hablemos de las listas de acceso.

La lista de acceso funciona como una lista de invitados a un restaurante o un evento. Aplica la misma lógica: si estás en la lista, entras. Si no, no entras. El técnico que desee conectar con un dispositivo que tenga habilitadas las listas de acceso deberá estar en la lista para que la conexión sea permitida. Si el técnico no está en la lista, la conexión será rechazada de inmediato.

Cuando tenemos grupos de trabajo grandes y muchos usuarios a quienes prestar servicio, la gestión de estas listas puede convertirse en un desafío. Imagínate tener 100 técnicos de servicio. Ahora piensa que a veces los técnicos dejan la empresa o llegan nuevos. Gestionar estas listas grandes puede representar mucho trabajo. Por eso se recomienda utilizar el espacio de nombres personalizado, de tal manera que cualquier identificador que esté dentro del espacio de nombres sea automáticamente incluido en la lista simplemente añadiendo ese espacio de nombres personalizado a la lista.

Las listas pueden contener identificaciones individuales, IDs numéricos, y comodines. Estos últimos son clave para una gestión dinámica y sencilla de la seguridad en grandes grupos. Te lo explico: al crear comodines, puedes formar grupos. Por ejemplo, tenemos tres grupos. Aquellos técnicos a los que queremos permitir acceso a los servidores de bases de datos. Los técnicos que tengan dentro de su identificador “Senior Tech” podrán conectar sin problema, y la única entrada que necesitarás agregar a tu ACL será el comodín `*Senior Tech`. Aquellos que pertenezcan a otros grupos, por su parte, no podrán conectar.

Si Lou, en este caso, deja la empresa, no podrá conectar a los dispositivos a los que anteriormente tenía acceso, incluso si conocía el ID y la contraseña de acceso. Por ello, es importante que consideres implementar las listas de control de acceso y adquirir un espacio de nombres personalizado para aumentar la seguridad de tu instalación y facilitar la gestión de seguridad en grandes grupos de soporte.