https://docs.ldap.com/ldap-sdk/docs/tool-usages/ldapsearch.html

La herramienta de línea de comandos ldapsearch

Procese una o más búsquedas en un servidor de directorios LDAP.

Los criterios para la solicitud de búsqueda se pueden especificar de varias maneras diferentes, incluido el suministro de todos los detalles directamente a través de argumentos de línea de comandos, el suministro de todos los argumentos excepto el filtro a través de argumentos de línea de comandos y la especificación de un archivo que contenga los filtros que se van a usar, o la especificación de un archivo que incluya un conjunto de direcciones URL LDAP con el DN base. ámbito, filtro y atributos que se van a devolver.

Consulte los ejemplos siguientes para ver una serie de líneas de comandos de ejemplo para esta herramienta.

**Uso**

ldapsearch *{arguments}* *{filter} [{attr1} [{attr2} ...]]*

**Argumentos de conexión y autenticación LDAP**

* -h *{host}* / --hostname *{host}* — La dirección IP o el nombre que se puede resolver para conectarse al servidor de directorios. Si no se proporciona, se utilizará un valor predeterminado de 'localhost'.
* -p *{port}* / --port *{port}* — El puerto que se usará para conectarse al servidor de directorios. Si no se proporciona, se utilizará un valor predeterminado de 389.  
  El valor especificado no debe ser inferior a 1 ni superior a 65.535.
* -D *{dn}* / --bindDN *{dn}* — El DN que se usará para enlazar al servidor de directorios al realizar la autenticación simple.  
  Un valor proporcionado debe poder analizarse como un nombre distintivo LDAP, tal como se describe en RFC 4514.
* -w *{password}* / --bindPassword *{password}* — La contraseña que se usará para enlazar al servidor de directorios cuando se realice una autenticación simple o un mecanismo SASL basado en contraseña.
* -j *{ruta}* / --bindPasswordFile *{ruta}* — La ruta al archivo que contiene la contraseña que se usará para enlazar al servidor de directorios al realizar una autenticación simple o un mecanismo SASL basado en contraseña.  
  La ruta de acceso especificada debe hacer referencia a un archivo que exista.
* --promptForBindPassword: indica que la herramienta debe solicitar interactivamente al usuario la contraseña de enlace.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -Z / --useSSL — Utilice SSL cuando se comunique con el servidor de directorios.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -q / --useStartTLS — Utilice StartTLS cuando se comunique con el servidor de directorios.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --defaultTrust: utilice el almacén de confianza predeterminado de la JVM y, opcionalmente, un almacén de confianza adicional especificado mediante el argumento --trustStorePath, para determinar de forma no interactiva si se debe confiar en cualquier cadena de certificados presentada durante la negociación TLS. Si no se puede confiar en la cadena en función de ninguna de esas fuentes, la negociación fracasará sin preguntar si se debe confiar en ella.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -X / --trustAll — Confía en cualquier certificado presentado por el servidor de directorios.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -K *{ruta}* / --keyStorePath *{ruta}* — La ruta de acceso al archivo que se usará como almacén de claves para obtener certificados de cliente cuando se comunique de forma segura con el servidor de directorios.
* -W *{password}* / --keyStorePassword *{password}* — La contraseña que se usará para acceder al contenido del almacén de claves.
* -u *{ruta}* / --keyStorePasswordFile *{ruta}* — La ruta de acceso al archivo que contiene la contraseña que se usará para acceder al contenido del almacén de claves.  
  La ruta de acceso especificada debe hacer referencia a un archivo que puede o no existir.
* --promptForKeyStorePassword: indica que la herramienta debe solicitar interactivamente al usuario la contraseña que se usará para acceder al contenido del almacén de claves.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --keyStoreFormat *{format}* — El formato (por ejemplo, JKS, PKCS12, PKCS11, BCFKS, etc.) para el archivo de almacén de claves.
* -P *{ruta}* / --trustStorePath *{ruta}* — La ruta de acceso al archivo que se usará como almacén de confianza al determinar si se debe confiar en un certificado presentado por el servidor de directorios.
* --trustStorePassword *{password}* — La contraseña que se usará para acceder al contenido del almacén de confianza.
* -U *{ruta}* / --trustStorePasswordFile *{ruta}* — La ruta de acceso al archivo que contiene la contraseña que se usará para acceder al contenido del almacén de confianza.  
  La ruta de acceso especificada debe hacer referencia a un archivo que puede o no existir.
* --promptForTrustStorePassword: indica que la herramienta debe solicitar interactivamente al usuario la contraseña que se va a utilizar para acceder al contenido del almacén de confianza.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --trustStoreFormat *{format}* — El formato (por ejemplo, JKS, PKCS12, PKCS11, BCFKS, etc.) para el archivo de almacén de confianza.
* --verifyCertificateHostnames: indica que la herramienta debe verificar que el nombre de host o la dirección IP utilizada para establecer conexiones con el servidor LDAP coincida con una dirección para la que se emitió el certificado TLS del servidor.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -N *{nickname}* / --certNickname *{nickname}* — El apodo (alias) del certificado de cliente en el almacén de claves que se va a presentar al servidor de directorios para la autenticación del cliente SSL.
* --enableSSLDebugging — Habilita el soporte de bajo nivel de Java para depurar la comunicación SSL/TLS. Esto equivale a establecer la propiedad 'javax.net.debug' en 'all'.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -o *{name=value}* / --saslOption *{name=value}* — Un par nombre-valor que proporciona información para usar al realizar la autenticación SASL.
* --useSASLExternal — Utilice el mecanismo SASL EXTERNAL para autenticarse.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --helpSASL — Proporciona información sobre los mecanismos SASL soportados, incluidas las propiedades disponibles para su uso con cada uno.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.

**Argumentos de la operación**

* -b *{dn}* / --baseDN *{dn}* — Especifica el DN base que se debe utilizar para la búsqueda. Si se proporciona un archivo de filtro, este DN base se utilizará para cada búsqueda con un filtro leído de ese archivo. Este argumento no debe proporcionarse si se proporciona --ldapURLFile. Si no se especifica ningún DN base, se utilizará el DN base nulo de forma predeterminada.  
  Un valor proporcionado debe poder analizarse como un nombre distintivo LDAP, tal como se describe en RFC 4514.
* -s *{base|one|sub|subordinates}* / --scope *{base|one|sub|subordinates}* — Especifica el ámbito que se va a utilizar para las solicitudes de búsqueda. El valor debe ser uno de 'base', 'one', 'sub' o 'subordinates'. Si no se proporciona este argumento, se usará un valor predeterminado de 'sub'.  
  El valor proporcionado debe ser uno de 'base', 'uno', 'sub' o 'subordinado'.
* -z *{value}* / --sizeLimit *{value}* — Especifica el número máximo de entradas que el servidor debe devolver para cada búsqueda. Un valor de cero (que es el valor predeterminado si no se utiliza este argumento) indica que no se debe imponer ningún límite de tamaño del lado cliente. Tenga en cuenta que el servidor puede imponer su propio límite en el número de entradas que se pueden devolver para una búsqueda.  
  El valor especificado no debe ser menor que 0 ni mayor que 2.147.483.647.
* -l *{value}* / --timeLimitSeconds *{value}* — Especifica el tiempo máximo en segundos que el servidor debe dedicar a procesar cada búsqueda. Un valor de cero (que es el valor predeterminado si no se proporciona este argumento) indica que no se debe imponer ningún límite de tiempo del lado cliente. Tenga en cuenta que el servidor puede imponer su propio límite de tiempo para las solicitudes de búsqueda.  
  El valor especificado no debe ser menor que 0 ni mayor que 2.147.483.647.
* -a *{never|always|search|find}* / --dereferencePolicy *{never|always|search|find}* — Especifica la política de desreferenciación de alias que se utilizará para las solicitudes de búsqueda. El valor debe ser 'nunca', 'siempre', 'buscar' o 'encontrar'. Si no se proporciona este argumento, se utilizará un valor predeterminado de 'never'.  
  Un valor proporcionado debe ser uno de los siguientes: 'always', 'never', 'search', 'find'.
* -A / --typesOnly: indica que el servidor solo debe incluir los nombres de los atributos contenidos en la entrada en lugar de nombres y valores.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --requestedAttribute *{attr}* — Especifica un identificador que indica qué atributo(s) deben incluirse en las entradas que coincidan con los criterios de búsqueda. El valor puede ser un nombre de atributo o OID, un token especial como '\*' para indicar todos los atributos de usuario o '+' para indicar todos los atributos operativos, o un nombre de clase de objeto precedido por un símbolo '@' para indicar todos los atributos asociados con la clase de objeto especificada. Esto se puede proporcionar varias veces para especificar varios atributos solicitados, y se puede proporcionar en lugar de o además del conjunto de atributos solicitados en el conjunto de argumentos finales. Si no se especifica, el servidor se comportará como si se hubieran solicitado todos los atributos de usuario.
* --filter *{filter}* — Especifica un filtro que se usará al procesar una búsqueda. Esto se puede proporcionar varias veces para emitir múltiples búsquedas con diferentes filtros. Si se proporciona este argumento, el primer argumento final no se interpretará como un filtro de búsqueda (todos los argumentos finales se interpretarán como atributos solicitados).  
  Un valor proporcionado debe poder analizarse como un filtro de búsqueda LDAP, como se describe en RFC 4515.
* -f *{ruta}* / --filterFile *{ruta}* — Especifica la ruta a un archivo que contiene los filtros de búsqueda que se van a emitir. Cada filtro debe estar en una línea separada. Las líneas en blanco y las líneas que comiencen con el carácter '#' serán ignoradas. Este argumento se puede proporcionar varias veces para especificar varios archivos de filtro. Si se proporciona un archivo de filtro, el primer argumento final no se interpretará como un filtro de búsqueda (todos los argumentos finales se interpretarán como atributos solicitados).  
  La ruta de acceso especificada debe hacer referencia a un archivo que exista.
* --ldapURLFile *{path}* — Especifica la ruta a un archivo que contiene URL LDAP que definen las solicitudes de búsqueda que se van a emitir. Las URL LDAP especificarán el DN base, el ámbito, el filtro y los atributos que se devolverán para cada búsqueda (se ignorarán los nombres de host y los números de puerto incluidos en las URL). Cada URL debe estar en una línea separada. Las líneas en blanco y las líneas que comiencen con el carácter '#' serán ignoradas. Este argumento se puede proporcionar varias veces para especificar varios archivos URL LDAP.  
  La ruta de acceso especificada debe hacer referencia a un archivo que exista.
* --followReferrals: intente seguir las referencias y las referencias de resultados de búsqueda encontradas durante el procesamiento de búsqueda. Si no se proporciona, las referencias y las referencias de búsqueda se mostrarán en la salida.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --retryFailedOperations: indica que, si se produce un error en una búsqueda de una manera que indica que la conexión con el servidor puede ya no ser válida, la herramienta debe crear automáticamente una nueva conexión y volver a intentar la búsqueda antes de notificarla como un error.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -c / --continueOnError — Continúa procesando búsquedas incluso si se encuentra un error. Si no se proporciona, el procesamiento se anulará después de la primera búsqueda fallida.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -r *{num}* / --ratePerSecond *{num}* — Especifica una velocidad de búsqueda máxima que la herramienta debe poder alcanzar. Tenga en cuenta que este límite solo se aplica a la velocidad a la que el cliente emite solicitudes de búsqueda y no a la velocidad a la que el servidor puede enviar entradas coincidentes.  
  El valor especificado no debe ser menor que 1 ni mayor que 2.147.483.647.
* --useAdministrativeSession: indica que la herramienta debe intentar utilizar una sesión administrativa para procesar todas las operaciones mediante un grupo dedicado de subprocesos de trabajo. Esto puede ser útil cuando se intenta diagnosticar problemas en un servidor que no responde porque todos los subprocesos de trabajo normales están ocupados procesando otras solicitudes.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -n / --dryRun — Indica qué búsquedas se emitirán, pero en realidad no las envía al servidor.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --countEntries — Indica que el código de salida de la herramienta debe representar el número de entradas devueltas durante el proceso de búsqueda. Si no se proporciona, o si se encuentra un error al procesar la búsqueda, el código de salida de la herramienta reflejará el código de resultado LDAP recibido durante el procesamiento de la búsqueda (o un código de resultado del lado del cliente adecuado si se encontró un problema antes de enviar cualquier búsqueda). Tenga en cuenta que debido a que algunos sistemas operativos no permiten valores de código de salida superiores a 255, ese será el valor de salida máximo para esta herramienta incluso si se devuelven más de 255 entradas. Tenga en cuenta también que este argumento solo se puede utilizar cuando se procesa una sola búsqueda.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.

**Argumentos de datos**

* --wrapColumn *{value}* — La columna en la que se deben ajustar las líneas largas en la representación LDIF de una entrada. Un valor de cero indica que no se debe realizar ningún ajuste. Si no se proporciona esto, la columna de ajuste se basará en el ancho del terminal utilizado para ejecutar la herramienta.  
  El valor especificado no debe ser menor que 0 ni mayor que 2.147.483.647.
* -T / --dontWrap: indica que no se debe realizar ningún ajuste de línea al mostrar las representaciones LDIF de las entradas coincidentes.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --suppressBase64EncodedValueComments: indica que la herramienta no debe incluir ningún comentario que intente proporcionar una representación legible de cualquier valor de atributo codificado en base64 en los resultados de la búsqueda. Si no se proporciona este argumento, cualquier valor de atributo cuya representación LDIF requiera codificación en base64 irá seguido inmediatamente de un comentario que intente proporcionar una representación legible de los bytes sin formato que componen ese valor codificado en base64.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --outputFile *{ruta}* — Especifica la ruta al archivo en el que se deben escribir los resultados de la búsqueda. Si no se proporciona este argumento, los resultados se escribirán en la salida estándar.  
  La ruta especificada debe hacer referencia a un archivo que puede o no existir, pero cuyo directorio principal debe existir.
* --compressOutput — Indica que la salida debe estar comprimida con gzip. Esto solo se puede usar si se proporciona el argumento --outputFile y no se proporciona el argumento --teeResultsToStandardOut.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --encryptOutput — Indica que la salida debe cifrarse con una clave generada a partir de una contraseña proporcionada. Esto solo se puede usar si se proporciona el argumento --outputFile y no se proporciona el argumento --teeResultsToStandardOut. Si se proporciona el argumento --encryptionPassphraseFile, ese archivo se usará para especificar la frase de contraseña de cifrado; de lo contrario, la frase de contraseña se solicitará de forma interactiva.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --encryptionPassphraseFile *{path}* — La ruta a un archivo que especifica la frase de contraseña que se va a utilizar para cifrar la salida. Esto solo se puede proporcionar si se proporciona el argumento --encryptOutput, pero si se proporciona ese argumento y no se especifica ningún archivo de frase de contraseña, se solicitará la frase de contraseña de forma interactiva. Si se especifica un archivo, ese archivo debe existir y debe contener exactamente una línea compuesta en su totalidad por la frase de contraseña.  
  La ruta de acceso especificada debe hacer referencia a un archivo que exista.
* --separateOutputFilePerSearch: indica que la herramienta debe generar un archivo de salida independiente para cada búsqueda en lugar de combinar todos los resultados en un solo archivo.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --teeResultsToStandardOut — Indica que los resultados de la búsqueda deben escribirse en la salida estándar, así como en el archivo de salida especificado a través del argumento 'outputFile'.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --outputFormat *{ldif|json|csv|multi-valued-csv|tab-delimited|multi-valued-tab-delimited|dns-only|values-only}* — Especifica el formato que se debe utilizar para la salida generada por esta herramienta. Los valores permitidos son 'LDIF' (formato de intercambio de datos LDAP, que es la representación de cadena estándar para los datos LDAP), 'JSON' (notación de objetos JavaScript, que es un formato popular utilizado por los servicios web), 'CSV' (valores separados por comas, que es un formato comúnmente utilizado para el procesamiento de texto, con un solo valor por atributo), 'multi-valued-csv' (valores separados por comas con una barra vertical entre los valores de los atributos multivalor), 'tabulado-delimitado' (otro formato de texto general de uso común, con un solo valor por atributo), 'multi-valued-tab-delimited' (texto delimitado por tabuladores con una barra vertical entre los valores de los atributos multivalor), 'dns-only' (en el que solo el DN de cada entrada coincidente se escribirá en una línea por sí misma sin información sobre los atributos de la entrada) y 'values-only' (en el que cada valor devuelto se escribirá en una línea por sí mismo sin nombres de atributos, DN de entrada, o delimitadores entre entradas). Si se selecciona el formato 'CSV' o 'delimitado por tabulaciones' (o una de sus variantes multivalor), el conjunto de atributos solicitados debe proporcionarse con el argumento '--requestedAttribute', el orden en el que se proporcionan los atributos en la línea de comandos especifica el orden en el que se enumerarán en la salida, y si alguno de esos atributos tiene varios valores, solo se utilizará el primer valor. Además, los formatos 'CSV' y 'delimitado por tabulaciones' no se pueden usar junto con el argumento '--ldapURLFile'. Si no se especifica ningún formato de salida, se utilizará un valor predeterminado de 'LDIF'.  
  Un valor proporcionado debe ser uno de los siguientes: 'values-only', 'multi-valued-csv', 'tab-delimited', 'ldif', 'csv', 'multi-valued-tab-delimited', 'json', 'dns-only'.
* --requireMatch — Indica que ldapsearch debe salir con un código de resultado distinto de cero, 94 (no se devuelven resultados), si la búsqueda se completa correctamente pero no devuelve ninguna entrada coincidente. Este argumento solo afecta al código de salida de la herramienta; no tendrá ningún efecto visible en la salida.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --terse — Indica que la herramienta debe generar una salida concisa. Lo único que se escribirá en la salida estándar serán las entradas de resultados de búsqueda y las referencias, sin ningún mensaje de resumen. El error estándar no se verá afectado.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -v / --verbose — Indica que la herramienta debe generar una salida detallada.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.

**Argumentos de control**

* --bindControl *{oid}[:{criticality}[:{stringValue}|::{base64Value}]]* — Especifica un control que debe incluirse en todas las solicitudes de enlace utilizadas para autenticarse en el servidor.  
  Un valor proporcionado debe ser una representación de cadena de un control LDAP válido con el formato {oid}[:{criticality}[:{stringValue}|::{base64Value}]].
* -J *{oid}[:{criticality}[:{stringValue}|::{base64Value}]]* / --control *{oid}[:{criticality}[:{stringValue}|::{base64Value}]]* — Especifica un control que debe incluirse en todas las solicitudes de búsqueda enviadas al servidor.  
  Un valor proporcionado debe ser una representación de cadena de un control LDAP válido con el formato {oid}[:{criticality}[:{stringValue}|::{base64Value}]].
* --accessLogField *{name:value}* — Indica que todas las solicitudes de búsqueda deben incluir un control de solicitud de campo de registro de acceso para indicar que el servidor debe incluir un campo personalizado con el nombre y el valor especificados. El nombre del campo debe contener solo letras, dígitos, guiones y guiones bajos ASCII. El nombre del campo debe ir seguido de dos puntos y el valor de campo de ese campo. Este argumento se puede proporcionar varias veces para solicitar varios campos de registro de acceso.
* --accountUsable: indica que todas las solicitudes de búsqueda deben incluir el control de solicitud utilizable de la cuenta propietaria de UnboundID para solicitar que cada entrada de resultado de búsqueda devuelta incluya un control de respuesta con información sobre el estado de usabilidad de la directiva de contraseñas para la entrada.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -E / --authorizationIdentity: indica que todas las solicitudes de enlace deben incluir el control de solicitud de identidad de autorización tal como se define en RFC 3829. Con este control, un resultado de enlace correcto debe incluir la identidad de autorización asignada a la conexión.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --assertionFilter *{filter}* — Un filtro que se usará junto con el control de solicitud de aserción LDAP (como se describe en RFC 4528) para indicar que el servidor solo debe procesar búsquedas en las que la entrada especificada como DN base coincida con este filtro.  
  Un valor proporcionado debe poder analizarse como un filtro de búsqueda LDAP, como se describe en RFC 4515.
* --excludeBranch *{dn}*: indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de exclusión de rama propietario de UnboundID para indicar que las entradas coincidentes por debajo del DN base especificado deben excluirse de los resultados de búsqueda. Este argumento se puede proporcionar varias veces si se deben excluir varias ramas.  
  Un valor proporcionado debe poder analizarse como un nombre distintivo LDAP, tal como se describe en RFC 4514.
* --generateAccessToken: indica que la solicitud de enlace debe incluir el control de solicitud de token de acceso generado, que se puede usar para solicitar que el servidor genere y devuelva un token de acceso que se pueda usar para autorizar conexiones posteriores a través del mecanismo SASL OAUTHBEARER.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --getAuthorizationEntryAttribute *{attr}* — Indica que todas las solicitudes de enlace deben incluir el control de solicitud de entrada de autorización get propietario de UnboundID para solicitar que el servidor devuelva el atributo especificado (o colección de atributos, en el caso de un identificador especial como '\*' para indicar todos los atributos de usuario o '+' para indicar todos los atributos operativos) de la entrada del usuario autenticado. Este argumento se puede proporcionar varias veces para especificar varios atributos para solicitar.
* --getBackendSetID: indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de ID de conjunto de back-end de UnboundID propietario de UnboundID para solicitar que el servidor proxy de directorio incluya un control de respuesta de ID de conjunto de back-end de obtención correspondiente en cada entrada de resultado de búsqueda, indicando el conjunto de back-end de equilibrio de entrada desde el que se recuperó esa entrada.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -g *{authzID}* / --getEffectiveRightsAuthzID *{authzID}* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud get effective rights propietario de UnboundID para devolver información sobre los derechos de control de acceso que tiene el usuario especificado al interactuar con cada entrada coincidente.
* -e *{attr}* / --getEffectiveRightsAttribute *{attr}* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud get effective rights propietario de UnboundID para devolver información sobre los derechos de control de acceso que tiene un usuario al interactuar con cada entrada coincidente. Este argumento se puede proporcionar varias veces para especificar varios atributos.
* --getRecentLoginHistory: indica que todas las solicitudes de enlace deben incluir el control de solicitud obtener historial de inicio de sesión reciente para solicitar que el servidor incluya un control de respuesta correspondiente con información sobre el historial de inicio de sesión reciente del usuario.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --getServerID: indica que todas las solicitudes de búsqueda deben incluir el control de solicitud get server ID propietario de UnboundID para solicitar que el servidor incluya un control de respuesta get server ID correspondiente en cada entrada de resultado de búsqueda, indicando el servidor desde el que se recuperó esa entrada.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --getUserResourceLimits: indica que todas las solicitudes de enlace deben incluir el control de solicitud get user resource limits propietario de UnboundID para solicitar que el servidor devuelva información sobre los límites de recursos (por ejemplo, límite de tamaño, límite de tiempo, límite de tiempo de inactividad, etc.) impuestos para el usuario.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --includeReplicationConflictEntries — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de entradas de conflicto de retorno de propiedad de UnboundID para indicar que el servidor puede devolver cualquier entrada de conflicto de replicación que coincida con los criterios de búsqueda. Normalmente, las entradas de conflicto de replicación se excluyen de los resultados de búsqueda.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --includeSoftDeletedEntries *{with-non-deleted-entries|without-non-deleted-entries|deleted-entries-in-undeleted-form}* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de acceso de entrada eliminada temporalmente propiedad de UnboundID para indicar que el servidor puede devolver cualquier entrada eliminada temporalmente que coincida con los criterios de búsqueda. Normalmente, las entradas eliminadas temporalmente se excluyen de los resultados de búsqueda. El valor de este argumento debe ser uno de los siguientes: 'with-non-deleted-entries' (indica que se deben devolver tanto las entradas normales como las eliminadas temporalmente), 'without-non-deleted-inputries' (indica que solo se deben devolver las entradas eliminadas temporalmente) o 'deleted-entries-in-undeleted-form' (devuelve solo las entradas eliminadas temporalmente en el formulario en el formulario que tenían las entradas antes de que se eliminaran).  
  Un valor proporcionado debe ser uno de los siguientes: 'with-non-deleted-entries', 'deleted-entries-in-undeleted-form', 'without-non-deleted-entryries'.
* --draftLDUPSubentries — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de subentradas como se describe en draft-ietf-ldup-subentry para indicar que el servidor puede devolver cualquier subentrada LDAP que coincida con los criterios de búsqueda. Normalmente, las subentradas LDAP se excluyen de los resultados de búsqueda. Este control no toma un valor.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --rfc3672Subentries *{returnOnlySubentries}* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de subentradas como se describe en RFC 3672 para indicar que el servidor puede devolver cualquier subentrada LDAP que coincida con los criterios de búsqueda, incluyendo opcionalmente entradas regulares junto con las subentradas. Normalmente, las subentradas LDAP se excluyen de los resultados de búsqueda. Este control requiere un valor booleano de 'true' o 'false' para indicar si el servidor debe devolver solo subentradas (si es verdadero) o tanto entradas normales como subentradas (si es falso).  
  Un valor proporcionado debe ser 'verdadero' o 'falso'.
* --joinRule *{dn:sourceAttr|reverse-dn:targetAttr|equals:sourceAttr:targetAttr|contains:sourceAttr:targetAttr }* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de unión para indicar que las entradas coincidentes deben unirse con entradas relacionadas en función de los criterios especificados. Los valores permitidos incluyen 'dn:' seguido del nombre de un atributo en la entrada de origen que contiene los DN de las entradas con las que se va a unir; 'reverse-dn:' seguido del nombre de un atributo en las entradas de destino cuyo valor es el DN de la entrada de origen; 'equals:' seguido del nombre de un atributo en la entrada de origen, dos puntos y el nombre de un atributo en las entradas de destino que debe coincidir exactamente con el atributo de origen; o 'contains:' seguido del nombre de un atributo en la entrada de origen, dos puntos y el nombre de un atributo en las entradas de destino que deben coincidir o contener el valor del atributo de origen.
* --joinBaseDN *{search-base|source-entry-dn|{ dn}}* — Especifica el DN base que se utilizará para las búsquedas utilizadas para unir las entradas de los resultados de la búsqueda con las entradas relacionadas. El valor puede ser uno de 'search-base' para usar el DN base de la solicitud de búsqueda, 'source-entry-dn' para usar el DN de la entrada de origen como DN base para las búsquedas de unión, o cualquier DN LDAP válido para usar un DN base personalizado para las búsquedas de unión. Si no se especifica, el DN base de unión predeterminado será el DN base de búsqueda.
* --joinScope *{base|one|sub|subordinates}* — Especifica el ámbito que se utilizará para las búsquedas utilizadas para unir las entradas de los resultados de búsqueda con las entradas relacionadas. El valor puede ser uno de 'base', 'uno', 'sub' o 'subordinados'. Si no se especifica, se usará el ámbito de la solicitud de búsqueda como ámbito de combinación.  
  El valor proporcionado debe ser uno de 'base', 'uno', 'sub' o 'subordinado'.
* --joinSizeLimit *{num}* — Especifica el número máximo de entradas que el servidor permitirá que se unan con cualquier entrada de resultado de búsqueda. Si no se proporciona, se utilizará el límite de tamaño de la solicitud de búsqueda. Tenga en cuenta que el servidor impondrá un límite máximo de tamaño de unión de 1000 entradas, por lo que cualquier límite de tamaño de unión superior a eso se limitará a 1000.  
  El valor especificado no debe ser menor que 0 ni mayor que 2.147.483.647.
* --joinFilter *{filter}* — Especifica un filtro adicional que el servidor requerirá que coincidan las entradas de destino para poder unirse a la entrada de origen. Si no se proporciona, no se utilizará ningún filtro de combinación adicional.  
  Un valor proporcionado debe poder analizarse como un filtro de búsqueda LDAP, como se describe en RFC 4515.
* --joinRequestedAttribute *{attr}* — Especifica un identificador que indica qué atributo(s) deben incluirse en las entradas unidas con las entradas de resultados de búsqueda. El valor puede ser un nombre de atributo o OID, un token especial como '\*' para indicar todos los atributos de usuario o '+' para indicar todos los atributos operativos, o un nombre de clase de objeto precedido por un símbolo '@' para indicar todos los atributos asociados con la clase de objeto especificada. Esto se puede proporcionar varias veces para especificar varios atributos solicitados. Si no se especifica, el servidor se comportará como si se hubieran solicitado todos los atributos de usuario.
* --joinRequireMatch — Indicates that the server should not return an entry that matches the search criteria if it is not joined with at least one additional entry. If this is not provided, then entries matching the search criteria will be returned even if they are not joined with any other entries.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* --manageDsaIT — Indicates that all search requests should include the manageDsaIT request control to indicate that any referral entries in the scope of the search should be treated as regular entries rather than causing the server to send search result references.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* --matchedValuesFilter *{filter}* — Indicates that all search requests should include the matched values request control (as described in RFC 3876) to indicate that search result entries should only include values for a given attribute that match the provided filter. This argument may be provided multiple times to specify multiple matched values filters.  
  A provided value must be able to be parsed as an LDAP search filter as described in RFC 4515.
* --matchingEntryCountControl *{examineCount=NNN[:alwaysExamine][:allowUnindexed][:skipResolvingExplodedIndexes][:fastShortCircuitThreshold=NNN][:slowShortCircuitThreshold=NNN][:extendedResponseData][:debug]}* — Indicates that all search requests should include the UnboundID-proprietary matching entry count request control, which indicates that the server should return information about the number of entries that match the search criteria. The maximum number of entries to examine must be specified, which helps indicate whether an exact count or an estimate will be returned. If alwaysExamine is specified and the number of candidates is less than the examine count, then each candidate will be examined to verify that it matches the criteria and would actually be returned to the client in a search. If allowUnindexed is specified, then the count will be allowed to be processed even if the search is unindexed (and may take a very long time to complete). If extended is specified, then the client will request extended response data from the server. If debug is specified, then additional debug information may be included in the output.
* --operationPurpose *{purpose}* — Indicates that all search requests should include the UnboundID-proprietary operation purpose request control to provide the specified reason for the operation.
* --overrideSearchLimit *{name=value}* — Indicates that search operations should include the override search limits request control with the specified name-value pair. This may be provided multiple times to specify multiple property name-value pairs to include in the control.
* -C *ps[:changetype[:changesonly[:entrychgcontrols]]]* / --persistentSearch *ps[:changetype[:changesonly[:entrychgcontrols]]]* — Indicates that the search request should include the persistent search request control (as described in draft-ietf-ldapext-psearch) to indicate that the server should return information about changes to entries that match the search criteria as they are processed. This argument may only be used when processing a single search operation.
* --permitUnindexedSearch — Indicates that all search requests should include the UnboundID-proprietary permit unindexed search request control to indicate that the server should process the search operation even if it cannot do so efficiently using server indexes. The requester must have either the unindexed-search or unindexed-search-with-control privilege.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* -Y *{authzID}* / --proxyAs *{authzID}* — Indicates that all search requests should include the proxied authorization request control (as described in RFC 4370) to process the operation under an alternate authorization identity. The authorization ID should generally be specified in the form 'dn:' followed by the target user's DN, or 'u:' followed by the username.
* --proxyV1As *{dn}* — Indicates that all search requests should include the legacy proxied authorization v1 request control (as described in draft-weltman-ldapv3-proxy-04) to process the search under an alternate authorization identity, specified as the DN of the desired user.  
  A provided value must be able to be parsed as an LDAP distinguished name as described in RFC 4514.
* --rejectUnindexedSearch — Indicates that all search requests should include the UnboundID-proprietary reject unindexed search request control to indicate that the server should not process the search operation if it cannot do so efficiently using server indexes, even if the requester has the unindexed-search privilege.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* --routeToBackendSet *{entry-balancing-processor-id:backend-set-id}* — Specifies the ID of an entry-balancing backend set to which the Directory Proxy Server should send all of the search requests. The value should be formatted as the entry-balancing request processor ID followed by a colon and the desired backend set ID for that entry-balancing request processor. This argument can be provided multiple times to specify multiple backend set IDs for the same or different entry-balancing request processors. The request control will be configured to use absolute routing rather than a routing hint.
* --routeToServer *{id}* — Specifies the ID of the backend server to which the Directory Proxy Server should send all search requests.
* --suppressOperationalAttributeUpdates *{attr}* — Indicates that all operations should include the UnboundID-proprietary suppress operational attribute updates request control to indicate that the server should not apply any updates to the specified operational attributes. The value may be one of 'last-access-time', 'last-login-time', 'last-login-ip', or 'lastmod'.  
  A provided value should be one of the following: 'last-access-time', 'last-login-ip', 'last-login-time', 'lastmod'.
* --usePasswordPolicyControl — Indicates that bind requests should include the password policy request control (as defined in draft-behera-ldap-password-policy-10) to request that the response include password policy-related information about the target entry.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* --realAttributesOnly — Indicates that all search requests should include the UnboundID-proprietary real attributes only request control to indicate that the server should not include any virtual attributes in entries that are returned.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* -S *{value}* / --sortOrder *{value}* — Indicates that all search requests should include the server-side sort request control (as described in RFC 2891) to request that the server sort results before returning them to the client. The sort order should be a comma-separated list of attribute names, each of which may be optionally prefixed by '+' (to indicate that sorting should be in ascending order for that attribute) or '-' (for descending order), and may be optionally followed by a colon and the name or OID for the ordering matching rule that should be used when sorting. Ascending order will be used if neither '+' or '-' is specified, and if no matching rule ID is given then the attribute type's own ordering rule will be used.
* --simplePageSize *{value}* — Indicates that all search requests should include the simple paged results control (as described in RFC 2696) to indicate that the search should return entries in pages of no more than the specified size. This can be useful for searches that must return a large number of entries but the server restricts the number of entries that may be returned for any search.  
  The specified value must not be less than 1 or greater than 2,147,483,647.
* --virtualAttributesOnly — Indicates that all search requests should include the UnboundID-proprietary virtual attributes only request control to indicate that the server should only include virtual attributes in entries that are returned.  
  This argument is not allowed to have a value. If this argument is included in a set of arguments, then it will be assumed to have a value of 'true'. If it is absent from a set of arguments, then it will be assumed to have a value of 'false'.
* -G *{before:after:index:count | before:after:value}* / --virtualListView *{before:after:index:count | before:after:value}* — Indica que todas las solicitudes de búsqueda deben incluir el control de solicitud de vista de lista virtual (VLV) (como se describe en draft-ietf-ldapext-ldapv3-vlv) para indicar que el servidor debe devolver el subconjunto especificado de los resultados de búsqueda ordenados (y también se debe dar el argumento 'sortOrder' para especificar el criterio de ordenación). El valor debe ser una lista delimitada por dos puntos que indique qué página de resultados se va a devolver, y puede adoptar una de estas dos formas. En cualquier caso, el primer elemento especifica el número de elementos que se devolverán antes de la entrada identificada como el inicio de los resultados, y el segundo es el número de entradas después de la entrada 'start'. El tercer elemento identifica el inicio del conjunto de resultados y puede ser un desplazamiento entero (en el que la primera entrada del conjunto de resultados tiene un desplazamiento de uno) o una cadena que proporciona un valor para el que el servidor debe identificar la primera entrada cuyo valor para el atributo de ordenación principal sea mayor o igual que la cadena dada. En el caso de que se proporcione un desplazamiento, también se debe dar un cuarto elemento para indicar el número esperado de entradas en el conjunto de resultados, o cero si no se conoce. Por ejemplo, un valor de '0:9:1:0' indica que el servidor debe devolver las diez primeras entradas del conjunto de resultados (empezando por el desplazamiento 1, que es la primera entrada, devuelve las cero entradas anteriores y las nueve entradas siguientes, sin indicación de cuántas entradas coinciden con los criterios de búsqueda). Como alternativa, un valor de '0:99:smith' indica que el servidor debe las primeras 100 entradas del conjunto de resultados para las que el atributo de ordenación principal tiene un valor mayor o igual que 'smith'.
* --useJSONFormattedRequestControls: indica que los controles de solicitud deben encapsularse en un control de solicitud con formato JSON. Incluso si de otro modo no hubiera ningún control de solicitud, se incluirá un control de solicitud con formato JSON vacío para indicar que el servidor debe encapsular los controles de respuesta en un control de respuesta con formato JSON.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.

**Argumentos de transformación de entrada**

* --excludeAttribute *{attr}* — Especifica el nombre o OID de un atributo que debe excluirse de las entradas de los resultados de búsqueda. Este argumento se puede proporcionar varias veces para especificar varios atributos que se van a excluir.
* --redactAttribute *{attr}* — Especifica el nombre o OID de un atributo cuyos valores deben redactarse para indicar que el atributo está presente en las entradas de los resultados de búsqueda, pero para ocultar los valores reales de ese atributo. Este argumento se puede proporcionar varias veces para especificar varios atributos para redactar.
* --hideRedactedValueCount — Indica que la salida no debe revelar el número de valores contenidos en los atributos redactados. Si este argumento está presente, entonces un atributo redactado solo tendrá un único valor de '\*\*\*REDACTED\*\*\*'. Si este argumento no está presente, entonces un atributo redactado con varios valores seguirá teniendo el mismo número de valores que tenía originalmente, pero esos valores serán '\*\*\*REDACTED1\*\*\*', '\*\*\*REDACTED2\*\*\*', etc.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --scrambleAttribute *{attr}* — Especifica el nombre o OID de un atributo cuyos valores deben ser aleatorizados. La aleatorización se realizará de una manera que intente conservar la sintaxis de atributo asociada y que, por lo general, intentará garantizar que un valor de entrada determinado produzca de forma coherente la misma salida aleatorizada. Este argumento se puede proporcionar varias veces para especificar varios atributos para codificar.
* --scrambleJSONField *{fieldName}* — Especifica el nombre de un campo JSON cuyos valores se deben codificar. Si se utiliza el argumento --scrambleAttribute para codificar cualquier atributo cuyos valores puedan ser objetos JSON, se conservarán todos los nombres de campo JSON y solo se codificarán los valores de los campos especificados. Si se proporciona este argumento (y se puede proporcionar varias veces para dirigirse a varios campos JSON), solo se codificarán los valores de los campos especificados. Si no se proporciona este argumento, cualquiera de los valores de atributo scramble que sean objetos JSON tendrá todos los valores codificados. Los nombres de campo JSON se tratarán sin distinguir entre mayúsculas y minúsculas.
* --scrambleRandomSeed *{value}* — Especifica el valor que se usará para inicializar el generador de números aleatorios utilizado en el curso de la aleatorización de valores de atributos. Si se proporciona una semilla aleatoria, la codificación de la misma entrada con la misma semilla debería producir consistentemente las mismas representaciones codificadas. Si no se especifica ningún valor de inicialización aleatorio, se seleccionará automáticamente un valor adecuado.  
  El valor especificado no debe ser inferior a -2.147.483.648 ni superior a 2.147.483.647.
* --renameAttributeFrom *{attr}* — Especifica el nombre o OID de un atributo cuyo nombre debe ser reemplazado por el valor especificado en el argumento --renameAttributeTo. Este argumento se puede proporcionar varias veces siempre que el argumento --renameAttributeTo también se proporcione el mismo número de veces, y el orden de los valores --renameAttributeFrom debe corresponder al orden de los valores --renameAttributeTo.
* --renameAttributeTo *{attr}* — Especifica el nuevo nombre que se usará para cambiar el nombre de un atributo. Este argumento debe proporcionarse el mismo número de veces que el argumento --renameAttributeFrom.
* --moveSubtreeFrom *{attr}* — Especifica el DN base para que un subárbol se mueva a otra ubicación en el DIT, con este DN de origen reemplazado por el DN base especificado mediante el argumento --moveSubtreeTo. Este argumento se puede proporcionar varias veces siempre que el argumento --moveSubtreeTo también se proporcione el mismo número de veces, y el orden de los valores de --moveSubtreeFrom debe corresponder al orden de los valores de --moveSubtreeTo.  
  Un valor proporcionado debe poder analizarse como un nombre distintivo LDAP, tal como se describe en RFC 4514.
* --moveSubtreeTo *{attr}* — Especifica el nuevo DN base para un subárbol que se va a mover. Este argumento debe proporcionarse el mismo número de veces que el argumento --moveSubtreeFrom.  
  Un valor proporcionado debe poder analizarse como un nombre distintivo LDAP, tal como se describe en RFC 4514.

**Argumentos adicionales**

* --scriptFriendly: indica que la herramienta debe funcionar en modo compatible con scripts. Este argumento no tiene ningún efecto y se proporciona solo con el fin de que sea compatible con otras herramientas ldapsearch.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -V *{value}* / --ldapVersion *{value}* — Especifica la versión del protocolo LDAP que la herramienta debe utilizar al comunicarse con el servidor de directorios. Este argumento no tiene ningún efecto y se proporciona solo con el fin de que sea compatible con otras herramientas ldapsearch.  
  El valor especificado no debe ser inferior a -2.147.483.648 ni superior a 2.147.483.647.
* --interactive — Inicia la herramienta en modo interactivo.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* -H / --help — Muestra la información de uso de este programa.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --version — Muestra la información de la versión de este programa.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --propertiesFilePath *{path}* — La ruta de acceso a un archivo de propiedades utilizado para especificar los valores predeterminados de los argumentos no proporcionados en la línea de comandos.  
  La ruta de acceso especificada debe hacer referencia a un archivo que exista.
* --generatePropertiesFile *{path}* — Escribe un archivo de propiedades vacío que se puede usar para especificar los valores predeterminados de los argumentos.  
  La ruta especificada debe hacer referencia a un archivo que puede o no existir, pero cuyo directorio principal debe existir.
* --noPropertiesFile — No obtiene ningún valor de argumento de un archivo de propiedades.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.
* --suppressPropertiesFileComment — Suprime la salida que enumera los argumentos obtenidos de un archivo de propiedades.  
  No se permite que este argumento tenga un valor. Si este argumento se incluye en un conjunto de argumentos, se asumirá que tiene un valor de 'true'. Si está ausente de un conjunto de argumentos, se asumirá que tiene un valor de 'false'.

**Conjuntos de argumentos dependientes**

* Si se proporciona el argumento --keyStorePassword, también se debe proporcionar el argumento --keyStorePath.
* Si se proporciona el argumento --keyStorePasswordFile, también se debe proporcionar el argumento --keyStorePath.
* Si se proporciona el argumento --promptForKeyStorePassword, también se debe proporcionar el argumento --keyStorePath.
* Si se proporciona el argumento --trustStorePassword, también se debe proporcionar el argumento --trustStorePath.
* Si se proporciona el argumento --trustStorePasswordFile, también se debe proporcionar el argumento --trustStorePath.
* Si se proporciona el argumento --promptForTrustStorePassword, también se debe proporcionar el argumento --trustStorePath.
* Si se proporciona el argumento --keyStorePath, también se debe proporcionar al menos uno de los siguientes argumentos: --useSSL, --useStartTLS
* Si se proporciona el argumento --trustStorePath, también se debe proporcionar al menos uno de los siguientes argumentos: --useSSL, --useStartTLS
* Si se proporciona el argumento --defaultTrust, también se debe proporcionar al menos uno de los siguientes argumentos: --useSSL, --useStartTLS
* Si se proporciona el argumento --trustAll, también se debe proporcionar al menos uno de los siguientes argumentos: --useSSL, --useStartTLS
* Si se proporciona el argumento --bindPassword, también se debe proporcionar al menos uno de los siguientes argumentos: --bindDN, --saslOption
* Si se proporciona el argumento --bindPasswordFile, también se debe proporcionar al menos uno de los siguientes argumentos: --bindDN, --saslOption
* Si se proporciona el argumento --promptForBindPassword, también se debe proporcionar al menos uno de los siguientes argumentos: --bindDN, --saslOption
* Si se proporciona el argumento --getEffectiveRightsAttribute, también se debe proporcionar el argumento --getEffectiveRightsAuthzID.
* Si se proporciona el argumento --virtualListView, también se debe proporcionar el argumento --sortOrder.
* Si se proporciona el argumento --separateOutputFilePerSearch, también se debe proporcionar el argumento --outputFile.
* Si se proporciona el argumento --separateOutputFilePerSearch, también se debe proporcionar al menos uno de los siguientes argumentos: --filter, --filterFile, --ldapURLFile
* Si se proporciona el argumento --teeResultsToStandardOut, también se debe proporcionar el argumento --outputFile.
* Si se proporciona el argumento --joinBaseDN, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --joinScope, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --joinSizeLimit, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --joinFilter, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --joinRequestedAttribute, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --joinRequireMatch, también se debe proporcionar el argumento --joinRule.
* Si se proporciona el argumento --hideRedactedValueCount, también se debe proporcionar el argumento --redactAttribute.
* Si se proporciona el argumento --scrambleJSONField, también se debe proporcionar el argumento --scrambleAttribute.
* Si se proporciona el argumento --scrambleRandomSeed, también se debe proporcionar el argumento --scrambleAttribute.
* Si se proporciona el argumento --renameAttributeFrom, también se debe proporcionar el argumento --renameAttributeTo.
* Si se proporciona el argumento --renameAttributeTo, también se debe proporcionar el argumento --renameAttributeFrom.
* Si se proporciona el argumento --moveSubtreeFrom, también se debe proporcionar el argumento --moveSubtreeTo.
* Si se proporciona el argumento --moveSubtreeTo, también se debe proporcionar el argumento --moveSubtreeFrom.
* Si se proporciona el argumento --compressOutput, también se debe proporcionar el argumento --outputFile.
* Si se proporciona el argumento --encryptOutput, también se debe proporcionar el argumento --outputFile.
* Si se proporciona el argumento --encryptionPassphraseFile, también se debe proporcionar el argumento --encryptOutput.

**Conjuntos de argumentos exclusivos**

* Los siguientes argumentos no se pueden usar juntos: --useSSL, --useStartTLS
* Los siguientes argumentos no se pueden usar juntos: --keyStorePassword, --keyStorePasswordFile, --promptForKeyStorePassword
* Los siguientes argumentos no se pueden usar juntos: --trustStorePassword, --trustStorePasswordFile, --promptForTrustStorePassword
* Los siguientes argumentos no se pueden usar juntos: --defaultTrust, --trustAll
* Los siguientes argumentos no se pueden usar juntos: --trustAll, --trustStorePath
* Los siguientes argumentos no se pueden usar juntos: --bindDN, --saslOption, --useSASLExternal
* Los siguientes argumentos no se pueden usar juntos: --bindPassword, --bindPasswordFile, --promptForBindPassword
* Los siguientes argumentos no se pueden usar juntos: --baseDN, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --scope, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --requestedAttribute, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --filter, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --filterFile, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --followReferrals, --manageDsaIT
* Los siguientes argumentos no se pueden usar juntos: --persistentSearch, --filterFile
* Los siguientes argumentos no se pueden usar juntos: --persistentSearch, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --draftLDUPSubentries, --rfc3672Subentries
* Los siguientes argumentos no se pueden usar juntos: --realAttributesOnly, --virtualAttributesOnly
* Los siguientes argumentos no se pueden usar juntos: --simplePageSize, --virtualListView
* Los siguientes argumentos no se pueden usar juntos: --terse, --verbose
* Los siguientes argumentos no se pueden usar juntos: --rejectUnindexedSearch, --permitUnindexedSearch
* Los siguientes argumentos no se pueden usar juntos: --wrapColumn, --dontWrap
* Los siguientes argumentos no se pueden usar juntos: --countEntries, --filter
* Los siguientes argumentos no se pueden usar juntos: --countEntries, --filterFile
* Los siguientes argumentos no se pueden usar juntos: --countEntries, --ldapURLFile
* Los siguientes argumentos no se pueden usar juntos: --countEntries, --persistentSearch
* Los siguientes argumentos no se pueden usar juntos: --compressOutput, --teeResultsToStandardOut
* Los siguientes argumentos no se pueden usar juntos: --encryptOutput, --teeResultsToStandardOut
* Los siguientes argumentos no se pueden usar juntos: --propertiesFilePath, --noPropertiesFile

**Ejemplos**

* Establece una conexión LDAP sin cifrar con directory.example.com:389, realiza un enlace simple para autenticarse como usuario 'uid=jdoe,ou=People,dc=example,dc=com', y emite una solicitud de búsqueda para recuperar los atributos givenName, sn y mail para el usuario con uid 'jqpublic' debajo de dc=example,dc=com. Los resultados de la búsqueda se escribirán en la salida estándar.

ldapsearch --hostname directory.example.com --port 389 \

--bindDN uid=jdoe,ou=People,dc=example,dc=com \

--bindPassword password --baseDN ou=People,dc=example,dc=com \

--scope sub "(uid=jqpublic)" givenName sn mail

* Establece una conexión LDAP cifrada con SSL para directory.example.com:636, preguntando de forma interactiva al usuario si debe confiar en el certificado presentado por el servidor de directorios. A continuación, la herramienta se enlazará con el mecanismo SASL PLAIN utilizando un ID de autenticación de 'u:jdoe' y una contraseña leída de un archivo. A continuación, emitirá una solicitud de búsqueda para cada filtro de un archivo determinado, escribiendo los resultados de cada búsqueda en un archivo de salida independiente.

ldapsearch --hostname directory.example.com --port 636 --useSSL \

--saslOption mech=PLAIN --saslOption authID=u:jdoe \

--bindPasswordFile /path/to/password/file \

--baseDN ou=People,dc=example,dc=com --scope sub \

--filterFile /path/to/filter/file \

--outputFile /path/to/base/output/file \

--separateOutputFilePerSearch --requestedAttribute '\*' \

--requestedAttribute "+"

* Establece una conexión LDAP con directory.example.com:389 que está protegida con la operación extendida StartTLS, utilizando la información del archivo de almacén de confianza proporcionado para determinar si se debe confiar en el certificado presentado por el servidor de directorios. A continuación, emitirá una búsqueda no autenticada para recuperar todos los atributos operativos y de usuario del DSE raíz del servidor. La salida se escribirá en un archivo de salida especificado y se mostrará en la salida estándar.

ldapsearch --hostname directory.example.com --port 389 --useStartTLS \

--trustStorePath /path/to/truststore/file --baseDN "" --scope base \

--outputFile /path/to/output/file \

--teeResultsToStandardOut '(objectClass=\*)' '\*' "+"

* Emite una solicitud de búsqueda para recuperar todas las entradas en o por debajo de 'dc=example,dc=com', utilizando el control de resultados paginados simple para recuperar hasta 100 entradas a la vez. La búsqueda utilizará una conexión LDAP sin cifrar, y la herramienta solicitará interactivamente al usuario la contraseña que debe utilizar al realizar una autenticación simple.

ldapsearch --hostname directory.example.com --port 389 \

--bindDN uid=admin,dc=example,dc=com --baseDN dc=example,dc=com \

--scope sub --outputFile /path/to/output/file --simplePageSize 100 \

'(objectClass=\*)' '\*' "+"

* Emite una solicitud de búsqueda para recuperar una entrada especial que proporciona detalles sobre el uso de índices por parte del servidor para determinar el conjunto candidato de posibles entradas coincidentes. Esta función solo se admite en el servidor de directorio de identidades UnboundID/Ping, y el usuario debe tener derechos de control de acceso para recuperar la entrada 'cn=debugsearch' y el atributo operativo 'debugsearchindex'.

ldapsearch --hostname directory.example.com --port 389 \

--bindDN uid=admin,dc=example,dc=com --baseDN dc=example,dc=com \

--scope sub "(&(givenName=John)(sn=Doe))" debugsearchindex

Descripción

Si el mandato **ldapsearch** encuentra una o varias entradas, se recuperan los atributos especificados por *atributos* y las entradas y valores se imprimen en la salida estándar. Si no se lista ningún *atributo*, se devuelven todos los atributos.

Distintivos

| **Nombre de distintivo** | **Descripción** |
| --- | --- |
| **-a** *desref* | Especifica cómo desreferenciar los alias (never, always, search o find). |
| **-A** | Recupera solo los nombres de atributos (no los valores). |
| **-b** *dn\_base* | Especifica el nombre distinguido (dn) base para la búsqueda. LDAP\_BASEDN del entorno es el valor predeterminado. |
| **-B** | Especifica no suprimir la impresión de los valores no ASCII. |
| **-C** *juego\_caracteres* | Establece el nombre del juego de caracteres que se utilizará, tal como se ha registrado con la Autoridad de números asignados por Internet (IANA). |
| **-d** *nivel* | Establece el nivel de depuración en la biblioteca LDAP. |
| **-D** *dn* | Enlace el dn. |
| **-e** | Muestra información de versión de la biblioteca LDAP y sale. |
| **-f***archivo* | Realiza una secuencia de búsquedas utilizando filtros en ‘archivo' “ debe sustituirse por el filtro. |
| **-F** *sep* | Imprime ‘sep' entre nombres de atributos y valores. |
| **-G** *reino* | Especifica que el reino debe utilizarse para el mecanismo de enlace DIGEST-MD5. |
| **-h** *host* | Especifica el nombre de host del servidor LDAP. |
| **-i** *archivo* | Realiza una secuencia de búsquedas utilizando filtros en ‘archivo' “ debe sustituirse por el filtro. |
| **-k** | Utiliza el control de administración de servidor en el enlace. |
| **-K** *archivo\_claves* | Especifica el archivo que se utilizará para las claves. |
| **-l** *tiempo* | Especifica el límite de tiempo (en segundos) para la búsqueda. |
| **-L** | Imprime entradas en formato LDIF (-B está implícito). |
| **-m***mecanismo* | Realiza el enlace SASL con el mecanismo especificado. |
| **-M** | Gestiona los objetos de referencia como entradas normales. |
| **-n** | Muestra lo que podría hacer pero en realidad no realiza la acción. |
| **-N***nombre\_clave* | Especifica el nombre de la clave privada que debe utilizarse en el archivo de claves. |
| **-o** *tipo\_atrib* | Ordena según el tipo de atributo especificado. |
| **-O***saltos\_máx* | Especifica el número máximo de referencias que deben seguirse en una secuencia. |
| **-p***puerto* | Especifica el número de puerto del servidor LDAP. |
| **-P***contraseña\_claves* | Especifica la contraseña del archivo de claves. |
| **-q** *tamaño\_página* | Consulta el tamaño de página para los resultados paginados. |
| **-R** | Especifica no seguir las referencias. |
| **-s***ámbito* | Ámbito de las búsquedas. El ámbito de la búsqueda puede ser uno de los siguientes: base, one o sub. |
| **-t** *ámbito* | Escribe valores en archivos en /tmp. |
| **-T** *segundos* | Especifica el número de segundos que hay que esperar entre páginas para los resultados paginados. |
| **-U** *nombre\_usuario* | Especifica el nombre de usuario para el mecanismo de enlace DIGEST-MD5. |
| **-v** | Se ejecuta en modalidad detallada. |
| **-V** ***versión*** | Especifica la versión del protocolo LDAP. La versión puede ser 2 ó 3. El valor predeterminado es 3. |
| **-w** *contraseña* | Enlaza la contraseña o '?' para una solicitud sin eco. |
| **-y** *dnproxy* | Establece el ID del proxy para la operación de autorización del proxy. |
| **-Y** | Utiliza una conexión LDAP segura (TLS). |
| **-z***tamaño* | Especifica el límite de tamaño (en entradas) para la búsqueda. |
| **-Z** | Utiliza una conexión LDAP segura (SSL). |
| **-9***control* | Establece la criticalidad de la opción de control. El control puede ser una de las siguientes opciones:   * **s**establece la criticalidad de ordenación en false * **p**establece la criticalidad de paginación en false |

Estado de salida

Consulte el apartado [Estado de salida para los mandatos del Servidor de E/S virtual](https://www.ibm.com/docs/es/POWER7/p7hcg/exit_status.htm#exit_status).

Ejemplos

Para abrir una conexión con el servidor LDAP y buscar en atributos específicos, escriba:

ldapsearch -h vclient.host.com -D cn=admin -w adminpw -b cn=aixdata objectclass=\*

Muestra del commando -h

ldapbúsqueda -h

ldapsearch: la opción requiere un argumento - 'h'

ldapsearch: opción no reconocida -h

uso: ldapsearch [opciones] [filtro [atributos...]]

dónde:

filtro Filtro de búsqueda LDAP compatible con RFC 4515

atributos lista de descripciones de atributos separadas por espacios en blanco

que puede incluir:

1.1 sin atributos

\* todos los atributos del usuario

+ todos los atributos operativos

Opciones de búsqueda:

-a deref uno de nunca (predeterminado), siempre, buscar o encontrar

-Recuperar solo nombres de atributos (sin valores)

-b basadon base dn para búsqueda

-c modo de operación continua (no se detiene ante errores)

-E [!]<ext>[=<extparam>] extensiones de búsqueda (! indica criticidad)

[!]accountUsability (usabilidad de la cuenta NetScape)

[!]domainScope (alcance del dominio)

!dontUseCopy (No usar copia)

[!]mv=<filtro> (filtro de valores coincidentes RFC 3876)

[!]pr=<tamaño>[/prompt|noprompt] (resultados paginados/mensaje RFC 2696)

[!]ps=<changetypes>/<changesonly>/<echg> (borrador de búsqueda persistente)

[!]sss=[-]<attr[:OID]>[/[-]<attr[:OID]>...]

(Clasificación del lado del servidor RFC 2891)

[!]subentradas[=true|false] (subentradas RFC 3672)

[!]sync=ro[/<cookie>] (solo actualización de sincronización LDAP RFC 4533)

rp[/<cookie>][/<slimit>] (refreshAndPersist)

[!]vlv=<antes>/<después>(/<desplazamiento>/<recuento>|:<valor>)

(vistas de lista virtual ldapv3-vlv-09)

[!]deref=derefAttr:attr[,...][;derefAttr:attr[,...][;...]]

!dirSync=<banderas>/<maxAttrCount>[/<cookie>]

(Sincronización de directorios de MS AD)

[!]extendedDn=<marca> (DN extendido de MS AD

[!]showDeleted (Mostrar MS AD eliminado)

[!]serverNotif (Notificación del servidor MS AD)

[!]<oid>[=:<value>|::<b64value>] (control genérico; sin manejo de respuestas)

-f operaciones de lectura de archivos desde `archivo'

-F prefijo Prefijo de URL para archivos (predeterminado: file:///tmp/)

-l límite de tiempo (en segundos, o "ninguno" o "máximo") para la búsqueda

-L imprimir respuestas en formato LDIFv1

-LL imprime respuestas en formato LDIF sin comentarios

-LLL imprime respuestas en formato LDIF sin comentarios

y versión

-M habilitar Administrar el control de TI de DSA (-MM para hacer crítico)

-P versión versión del protocolo (predeterminado: 3)

-s alcance uno de base, uno, sub o hijos (alcance de búsqueda)

-S attr ordena los resultados por atributo `attr'

-t escribir valores binarios en archivos en el directorio temporal

-tt escribe todos los valores en archivos en el directorio temporal

-T ruta escribe archivos en el directorio especificado por ruta (predeterminado: /tmp)

-u incluye nombres de entrada fáciles de usar en la salida

-z límite de tamaño (en entradas, o "ninguno" o "máximo") para la búsqueda

Opciones comunes:

-d nivel establece el nivel de depuración LDAP en 'nivel'

-D enlazar enlazar DN

-e [!]<ext>[=<extparam>] extensiones generales (! indica criticidad)

[!]assert=<filtro> (RFC 4528; una cadena de filtro RFC 4515)

[!]authzid=<authzid> (RFC 4370; "dn:<dn>" o "u:<usuario>")

[!]bautzid (RFC 3829)

[!]encadenamiento[=<resolveBehavior>[/<continuationBehavior>]]

uno de "chainingPreferred", "chainingRequired",

"referenciasPreferidas", "referenciasRequeridas"

[!]administrarDSAit (RFC 3296)

[!]noop

política

[!]postread[=<attrs>] (RFC 4527; lista de atributos separados por comas)

[!]preread[=<attrs>] (RFC 4527; lista de atributos separados por comas)

[!]relajarse

[!]seguimiento de sesión[=<nombre de usuario>]

abandonar, cancelar, ignorar (SIGINT envía abandonar/cancelar,

o ignora la respuesta; si es crítico, no espera a SIGINT.

realmente no controla)

-H URI Identificadores uniformes de recursos LDAP

-Utilizo el modo interactivo SASL

-n mostrar lo que se haría pero en realidad no lo hagas

-N no utilice DNS inverso para canonicalizar el nombre de host SASL

-O props propiedades de seguridad SASL

-o <opt>[=<optparam>] cualquier opción de libldap ldap.conf, más

ldif\_wrap=<ancho> (en columnas, o "no" para no ajustar)

nettimeout=<tiempo de espera> (en segundos, o "ninguno" o "máximo")

-Q usar el modo silencioso SASL

-R reino reino SASL

-U authcid identidad de autenticación SASL

-v ejecutar en modo detallado (diagnóstico a salida estándar)

-V información de la versión impresa (solo -VV)

-w passwd vincular contraseña (para autenticación simple)

-W solicita contraseña de enlace

-x Autenticación simple

-X authzid Identidad de autorización SASL ("dn:<dn>" o "u:<usuario>")

-y archivo Leer contraseña del archivo

-Y mecanismo SASL mecánico

-Z Iniciar solicitud TLS (-ZZ para requerir una respuesta exitosa)