Universidad de Costa Rica

Escuela de Ciencias de la Computación e Informática

CI0121 Redes de Comunicación de Datos

Proyecto de Investigación

Servicios de Red: LDAP y AD

Profesor:
Jose Antonio Brenes Carranza

Estudiantes:

Jorge Ignacio Chavarría Herrera	B82073
Sergio José Martínez Calvo	B84621
Kevin Reyes Solano	B86536
Joseph Sosa Quesada	B87757

II Semestre

2020

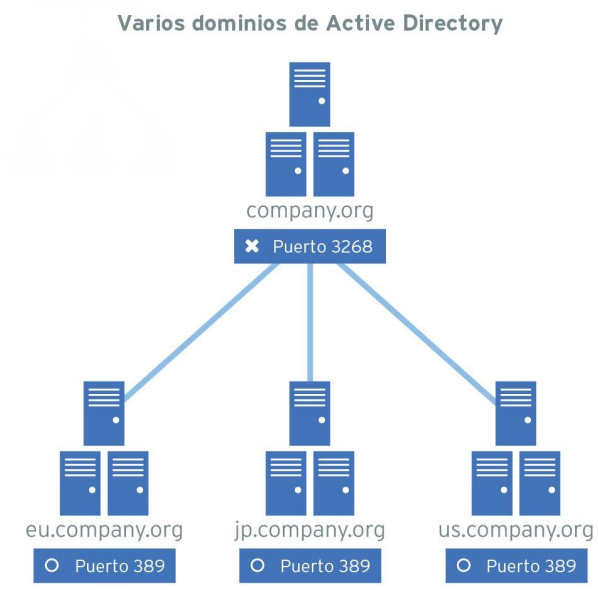
1. Directorio Activo (AD)

El Directorio Activo de Microsoft Windows, consiste en una estructura informática de base de datos, que desglosa de manera jerárquica la información de la infraestructura. Esto con el fin de permitir a un administrador en tecnologías de la información, administrar y gestionar recursos y servicios de los equipos y la red. Además permite localizar, proteger y administrar los usuarios, grupos, archivos, dispositivos periféricos y de red en la infraestructura. Al ser un recurso de tipo base de datos, lleva registro de la información más sensible y compartida como los permisos de los archivos, las contraseñas de los usuarios, los dispositivos periféricos conectados y sus respectivas tareas y acciones.

El directorio activo funciona a partir de tres conceptos de suma importancia. Por un lado, el dominio, que consiste en un conjunto de ordenadores conectados a una red, es el objeto principal del directorio activo, dado que es el componente principal de la estructura, ya que sin el dominio, no se puede manejar el directorio activo como una estructura jerárquica. Por otro lado, existen los subdominios, los cuales corresponden a dominios de tipo segundo nivel, en donde, sigue la estructura jerárquica teniendo en cuenta que el dominio es el principal. Estos tienen como objetivo la distribución ordenada de la información a lo interno de la infraestructura, no almacenar o representar la infraestructura de una manera caótica. Por otra parte,

existe el concepto de árbol que representa un conjunto de dominios que dependen de una raíz común, al mismo tiempo está el bosque, donde se tiene que un bosque es la infraestructura donde se tiene más de un dominio y estos se relacionan entre sí. Toda la información representada o derivada de los dominios relacionados, corresponde a un bosque en el directorio activo.

Dado que el directorio activo tiene tal estructura, es posible interpretar que con la representación de tipo jerárquica, la infraestructura es mucho más ordenada y los planeamientos y cambios son sumamente sencillos. Por ejemplo, se pueden representar grupos de usuarios o servidores en diversos subconjuntos, donde exista esa separación lógica en la infraestructura y el directorio activo sea realmente aprovechado.



Con tal estructura lógica en el directorio activo, se pueden dar acciones, gestiones y servicios a lo interno del directorio de tipo creación de un grupo conformado por ciertos usuarios, dar privilegios específicos a ciertos grupos de usuarios o incluso a usuarios más específicos. Además, permite manejar la autenticación a niveles de seguridad en el dominio, solo dejando a usuarios con permisos ingresar al sistema; estos usuarios, están almacenados en este directorio activo y no en cada computadora conectada al servidor.

En cuanto a los servicios de red, el Directorio Activo o AD, por sus siglas en inglés, es una herramienta para el uso de servicios de directorio de Microsoft, lo que significa que se puede usar para administrar múltiples equipos en una red. En estos equipos se pueden gestionar los usuarios, así como las credenciales de estos, la instalación de programas o el acceso remoto.

Además, AD utiliza los protocolos de red LDAP, DHCP, KERBEROS y DNS. Al lado de estos protocolos es necesario tener el protocolo TCP/IP con una dirección de IP fija configurada en equipo que actuará como servidor, un servidor DNS y el sistema operativo Windows Server por lo que Linux y otras versiones de Windows no pueden usar esta herramienta.

1.1 Controlador de dominio

Es un servidor de Windows que guarda una copia de la cuenta e información de seguridad de un dominio y permite definir los límites de este. Con un controlador de dominio se puede dar y quitar acceso, administrar recursos informáticos o dispositivos entre otras funciones.

1.2 Puertos

Para poder implementar un AD correctamente se necesitan habilitar ciertos puertos, aunque también esta la opcion de usar IPSec o DMZ pero no es lo recomendado, los puertos necesarios son:

RPC endpoint mapper: puerto 135 TCP, UDP

NetBios name service: puerto 137 TCP, UDP

NetBIOS datagram service: puerto 138 UDP

NetBIOS session service: puerto 139 TCP

SMB por IP (Microsoft-DS): puerto 445 TCP, UDP

LDAP: puerto 389 TCP, UDP

LDAP por SSL: puerto 636 TCP

Global catalog LDAP: puerto 3268 TCP

Global catalog LDAP over SSL: puerto 3269 TCP

Kerberos: puerto 88 TCP, UDP

DNS: puerto 53 TCP, UDP

WINS resolution: puerto 1512 TCP, UDP

WINS replication: puerto 42 TCP, UDP

RPC: Puertos alocados dinámicamente TCP

1.3 Seguridad de AD

La seguridad del Directorio Activo es imprescindible para proteger las credenciales de los usuarios, los sistemas computacionales de las compañías, datos o información sensible, aplicaciones de usuarios, accesos no autorizados y principalmente los tres pilares de la seguridad de la información: disponibilidad, integridad y confidencialidad. En el caso de que se comprometa la seguridad de la información de un Directorio Activo, la información pasa a ser completamente vulnerable y esto puede llevar a niveles catastróficos del filtrado de la información del mismo Directorio Activo e incluso a corrupción o destrucción de los sistemas computacionales.

El Directorio Activo es en gran parte la división de usuarios autorizados y los no autorizados, el acceso y los diferentes permisos por usuario y por grupos de usuarios, las aplicaciones en la organización y sus diferentes permisos. En general, conecciones y permisos los cuales, si el Directorio Activo llega a ser vulnerable por un ataque, probablemente las cuentas de usuarios, bases de datos internas, aplicaciones y cualquier tipo de información en el mismo, puedan ser accedidas y

filtradas; provocando una exposición gigantesca de la información de la cual sería extremadamente difícil recuperarse.

Entre las vulnerabilidades más comunes se encuentra dejar las configuraciones de seguridad predeterminadas, ya que estas no se acoplan perfectamente a las necesidades de todas las organizaciones y además estas configuraciones son las que los hacker conocen. Otro problema común corresponde a privilegios de superusuario dados a usuarios que no deberían tenerlos. Lo mismo puede suceder con permisos a diferentes aplicaciones o a la misma información. Además, también se cuenta con las vulnerabilidades más comunes, contraseñas fáciles y software no actualizado el cual evita corregir errores en el sistema.

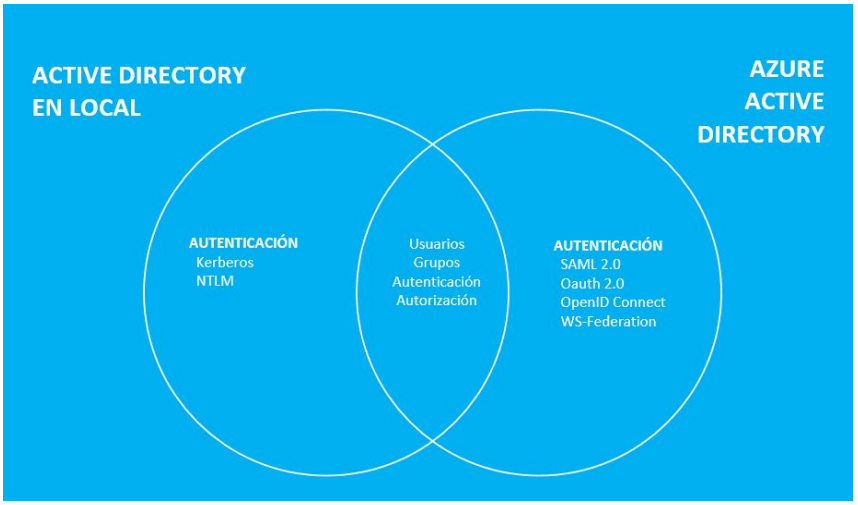
Dadas tales definiciones de las vulnerabilidades más conocidas, las mejores prácticas para mantener seguro el Directorio Activo de Windows incluye revisar y modificar constantemente las configuraciones de seguridad y relacionarlas al propósito del Directorio Activo, tomar en cuenta la importancia de los usuarios y los grupos de usuario, así como sus permisos de uso y de superusuario principalmente. Por otro lado, también es significante tener una copia externa de los sistemas, tener alertas activas para verlas al instante y constantemente actualizar el software con el fin de brindar parches a posibles vulnerabilidades de seguridad en el sistema.

1.4 Directorio Activo en la Nube

Por otro lado, existe el Directorio Activo Azure, un servicio de administración de identidades, basado en la nube o la cloud de Microsoft. La cual, al igual que un Directorio Activo, permite crear usuarios y grupos para acceder a aplicaciones y a su vez, administrar.

Mientras el Directorio Activo utiliza protocolos como Kerberos y NTLM para la autenticación y LDAP para consultar y modificar elementos en la base de datos, el Directorio Activo Azure utiliza protocolos basados en la nube como SAML y OAuth, así como una APIs de Transferencia de Estado Representacional para la comunicación.

Una gran diferencia entre el Directorio Activo local y el de Azure es que en esta última no se utilizan bosques ni dominios, siendo un diseño en la nube que abarca todo, es decir, lo que se administra es la organización completa. No hay separaciones ni una estructura jerárquica. En cuanto a diferencias, las anteriormente mencionadas son las principales, dado que la función es muy parecida, es evidente que los principales cambios son dados en cuanto a la implementación.



2. Lightweight Directory Access Protocol (LDAP)

El protocolo ligero de acceso a directorios es un protocolo que surgió en 1995 como respuesta al protocolo de acceso a directorio(DAP). El modelo del protocolo se basa en un cliente que transmite una solicitud con la descripción de la operación que se desea ejecutar en el servidor. Seguidamente el servidor se encarga de ejecutar estas operaciones.

Según Yeong, Howes y Killes (1995) el objetivo de implementar este protocolo en lugar de DAP es abaratar los costos asociados con el uso del directorio X.500, así como permitir mayor aplicaciones que lo usen reduciendo la complejidad de los clientes. Como LDAP es un protocolo para el acceso al directorio X.500 necesita algún servicio que pueda garantizar una conexión confiable, por este motivo es común implementarlo con el servicio TCP utilizando el puerto 389. El puerto 389 se usa para manejar queries de autentificación de clientes. Yeong, Howes y Killes (1995) exponen que para trabajar con el servicio COTS no se realiza ningún uso especial de T-Connect ya que es mapeado directamente a T-Data.

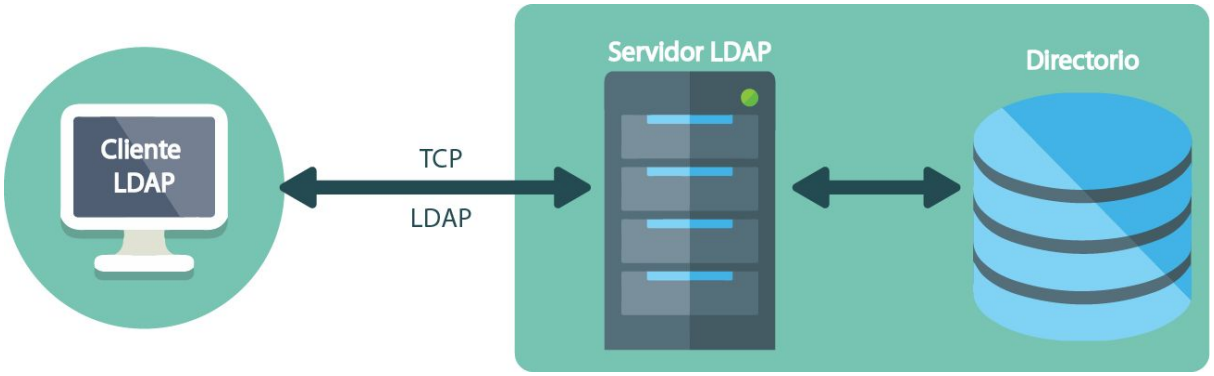
Los mensajes en LDAP siguen una estructura la cual posee 2 atributos; el primero es el ID del mensaje, este es un número entero y debe ser único a lo largo de toda la sesión de la que forma parte. El segundo atributo es la operación que se le desea solicitar al servidor. Yeong, Howes y Killes (1995) definieron 16 operaciones distintas: bindRequest, bindResponse, unbindRequest, searchRequest, searchResponse, modifyRequest, modifyResponse, addRequest, addResponse, delRequest, delResponse, modifyRDNRequest, modifyRDNResponse, compareDNRequest, compareDNResponse, abandonRequest. Es importante aclarar que el ID original del mensaje debe mantenerse en cualquier respuesta correspondiente a la solicitud original.

Al igual que con el mensaje enviado la respuesta que da el servidor también debe ir encapsulada en una estructura específica, esta se compone de 3 atributos distintos, el primero siendo el código de resultado, este código es un número que va del 0 al 80, donde 0 indica éxito y cualquier otro número indica un fallo; cabe destacar que cada código de fallo indica un error distinto. Además tiene cual es el

distinguished name correspondiente y tiene un LDAPString para indicar el mensaje de error.

Como LDAP se conecta al directorio OSI (directorio X.500) es necesario definir una representación para el Nombre Distinguido y el Nombre Distinguido Relativo. Es por esto que existe el LDAPDN y RelativeLDAPDN y ambos están definidos por LDAPString, el cual es un es un string del tipo Octet String. Kille (1995) expone que los nombres distinguidos son utilizados en el directorio OSI como la llave primaria para las entradas del directorio.

El LDAP está diseñado para que los clientes se comuniquen con un servidor LDAP, que es el que se encarga de resolver las consultas LDAP del cliente comunicándose con el directorio al que se desea acceder, para luego devolver la respuesta al cliente.



2.1 Operaciones del protocolo LDAP

Como se denota anteriormente las operaciones que posee un mensaje del protocolo pueden ser agrupadas 9 divisiones específicas

- Bind Operation:

Esta es una operación que se encarga de iniciar la sesión del protocolo entre un cliente y un servidor; es por este motivo que debe ser la primera operación que

se ejecuta y se encuentra encapsulada en una estructura que contiene la versión, la cual es un entero, el distinguished name y que tipo de autenticación, este último es un LDAPString. Yeong, Howes y Killes (1995) indican que existen tres tipos de autenticación donde la primera (simple) provee el mínimo de permisos, y se puede utilizar para conexiones anónimas. Las otras dos opciones utilizan las opciones de autenticación Kerberos versión 4. Sin embargo en versiones más nuevas estas opciones se ven reemplazadas por los mecanismos SASL. Finalmente la respuesta del servidor solo indica el estatus de la solicitud.

- Unbind Operation:

Esta operación se debe realizar al final y es la encargada de terminar la sesión. No presenta una respuesta ya que el cliente asume que la sesión fue terminada y el servidor asume que el cliente terminó la sesión y la descarta.

- Search Operation:

La operación Search le permite al cliente solicitar una búsqueda al servidor. Esta operación necesita el Distinguished name que va a funcionar como el objeto base, un indicador del alcance de la búsqueda, un indicador de cómo manejar los alias de los objetos; Yeong, Howes y Killes (1995) definieron 4 valores posibles para este indicador: neverDerefAliases, derefInSearching, DerefFindingBaseObject y derefAlways, ademas del límite de tamaño y tiempo así como qué atributos debe contener el resultado, así como un filtro con las condiciones deseadas y los atributos de las entradas encontradas.

Al igual que la operación Bind esta cuenta con una estructura para la respuesta; esta estructura contiene el Distinguished name, la cantidad de entradas encontradas en la búsqueda, esto incluye aún cuando no se encuentra ninguna entrada y finalmente el código de resultado.

- Modify Operation:

Modify permite al cliente solicitar al servidor modificaciones en el directorio para esto es necesario el Distinguished name correspondiente y que tipo de

modificación. Yeong, Howes y Killes (1995) asignaron 3 operaciones distintas a la modificación de modo que se necesita el tipo de operación (add, delete o replace), el tipo de atributos a modificar y los valores que se desean.

De forma similar al bind el servidor envía una respuesta simple al cliente indicando si la modificación fue exitosa o si se dio algún error en el proceso.

- Add Operation:

Esta operación permite al cliente solicitar que se añada una entrada al directorio, los parámetros necesarios para ejecutarla son el Distinguished Name de la entrada a añadir, y una lista de los atributos que conformarán esta entrada. La respuesta del servidor indica si se pudo añadir o no la entrada al directorio por medio del Add Response.

- Delete Operation:

La operación de borrado permite que el cliente pida la eliminación de una de la entradas del directorio (únicamente para los datos hojas del directorio), para lo que requiere el Distinguished Name de la entrada a borrar como único parámetro. A través del Delete Response el servidor indica si la entrada fue borrada o si se produjo un error.

- Modify RDN Operation:

Esta operación permite al cliente modificar el último componente del nombre de una entrada del directorio, para lo que necesita el nombre de la entrada a modificar, el RDN que formará el último componente del nuevo nombre y un booleano que indique si los atributos modificados deberán ser eliminados o guardados como parte de la entrada. El resultado de la operación será devuelto al cliente a través de Modify RDN Response.

- Compare Operation:

La operación de comparación se utiliza para saber si una entrada del directorio contiene un valor específico en un atributo, para lo que se necesita el

nombre de la entrada, el nombre del atributo y su valor a comparar. El resultado de la comparación y su estado (exitoso o con errores) se envían por medio del Compare Response.

- Abandon Operation:

Esta operación se utiliza para que el cliente solicite que el servidor termine una operación que esté ejecutando, para lo que se necesita enviar el ID de la operación a detener. La operación de abandono no retorna nada indicando si fue exitosa, sólo se tiene que esperar que la operación fue detenida. Si el server recibe un Abandon Operation mientras está realizando un Search Operation, el server deberá terminar inmediatamente cualquier transmisión que esté enviando para realizar la búsqueda.

2.2 Puertos utilizados en LDAP

El protocolo ligero de acceso a directorios utiliza el puerto 389, y el 636 para la versión segura, ambos funcionan bajo el protocolo de transporte TCP, el cual necesita el 3-way-handshake para verificar la conexión adecuada entre el emisor y el receptor, o también bajo UDP, el cual no verifica que los paquetes lleguen correctamente, dando prioridad a la velocidad de entrega del mensaje.Estos puertos están reservados únicamente para este servicio.

2.3 Seguridad en LDAP

Dado que LDAP surgió como una versión más ligera del protocolo DAP que se utilizaba para el acceso al directorio X.500, después de todo su nombre lo indica, utiliza algunos métodos de seguridad que utilizaba el protocolo original. Sin embargo Hassler (1999) expone que el protocolo DAP sólo buscaba proteger la acción de bind mientras que LDAP busca proteger todas las operaciones subsecuentes de esa sesión, exceptuando claro la operación unbind que como ya se vió anteriormente no requiere de ningún tipo de autentificación.

Ya que LDAP busca proteger todas las operaciones es necesario determinar cuales son los posibles casos y las posibles vulnerabilidades en cada una de las operaciones:

- En el caso de las operaciones Bind y Unbind como se pueden tener usuarios anónimos se tiene el riesgo de que estos entren al sistema y consigan información sensible. Para esto Hassler (1999) presenta la necesidad de un servicio de autenticación de entidad donde el cliente autentifica al servidor y el servidor al cliente.
- La lectura del directorio requiere que el usuario tenga derechos de lectura para la entrada específica que busca leer. El mayor problema en este caso es que un atacante consiga la contraseña de un usuario y utilice estas credenciales para extraer información sensible. A raíz de eso en estos casos se implementa autenticación basada en algoritmos de llave pública Hassler (1999) .
- Cuando se implementa una operación de búsqueda surge el mismo problema que en los casos de lectura, sin embargo hay que tomar en cuenta que aquí es necesarios asignar permisos para realizar filtraciones o comparaciones.
- Finalmente las modificaciones del directorio son las que requieren un proceso de autenticación más fuerte ya que pueden cambiar la información del directorio.

Cuando se trata de la protección de las consultas y las respuestas hay 2 aspectos importantes a tomar en cuenta; el primero es que el servidor necesita confirmar que la solicitud viene de un cliente específico y el cliente debe estar seguro de la autenticidad, integridad y confidencialidad de los datos. Esto solo se logra estableciendo una conexión segura, como el caso de DAP; o protegiendo cada operación, como el caso de LDAP.

Como es mencionado anteriormente en estos protocolos hay 3 tipos de autenticación de usuarios: No autenticación, autenticación simple y autenticación fuerte. La primera es utilizada para los usuarios anónimos, la segunda se utiliza cuando no hay riesgo de que se filtre información sensible y la última es la utilizada

cuando hay operaciones de escritura o se manejan consultas de información sensible. Para poder implementar la última es necesario usar un elemento externo como una llave pública.

Finalmente para proteger las operaciones al directorio, LDAP implementa 3 operaciones de firma como parámetros de seguridad en sus consultas, estas son: SignedOperation, DemandSignedResult y SignedResult. SignedOperation contiene la firma del servidor o una solicitud para que el servidor firme la solicitud; DemandSignedResult es un booleano que indica si el servidor debe firmar la solicitud y finalmente si el servidor puede firmar envía el atributo SignedResult con la firma respectiva.

2.4 Configuración del servidor

Para configurar un servidor que utilice el protocolo LDAP es necesario el URL que indica la localización del servidor, el LDAP DN y las credenciales del administrador y una vez que se tienen estos datos ya se puede iniciar con la creación de usuarios y grupos.

Bibliografía:

Active Directory Security. (2020). BeyondTrust.

https://www.beyondtrust.com/resources/glossary/active-directory-security

Active Directory: definición y detalles. (s.f.). PAESSLER.

https://www.es.paessler.com/it-explained/active-directory

Castillo, J. A. (2018, diciembre 18). *Active Directory Qué es y para qué sirve*. Profesional Review.

https://www.profesionalreview.com/2018/12/15/active-directory/

Configuración de Active Directory. (2020). Trend Micro.

https://docs.trendmicro.com/es-es/smb/worry-free-business-security-services-67-server-help/administering/active-directory-set_001.aspx

Hassler. V., (1999). "*X.500 and LDAP security: a comparative overview*". IEEE Network, November 1999, Vol.13(6), pp.54-64. Recuperado de

https://juancenteno.info/controlador-dominio-windows/

Juan. (2017, February 16). *controlador de dominio en Windows*. Juan Centeno.

https://juancenteno.info/controlador-dominio-windows/

Kille, S., "*A String Representation of Distinguished Names*", RFC 1779, ISODE Consortium, March 1995. Recuperado de: https://tools.ietf.org/html/rfc1779

Manage Engine. (2020). ADManager Plus.

https://www.manageengine.com/es/ad-manager/

Petters, J. (2020, junio 17). *What is an Active Directory Forest?* Varonis.

https://www.varonis.com/blog/active-directory-forest/

Service Name and Transport Protocol Port Number Registry. (s. f.). iana.org. Recuperado el 20 de septiembre de 2020, de https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=ldap

Tinas, E. G. (2020). *Cloud Center Andalucía*. Windows Active Directory o Azure AD, ¿que hacer? https://www.cloudcenterandalucia.es/blog/windows-active-directory-o-azure-ad-que-hacer/

Yeong, W., Howes, T., Kille S., "*Lightweight Directory Access Protocol*", RFC 1777, Performance Systems International, University of Michigan, ISODE Consortium, March 1995. Recuperado de: https://dl.acm.org/doi/pdf/10.17487/RFC1777

Zeltser, L (2009, octubre 27). Cyber Security Awareness Month - Day 27 - Active Directory Ports https://isc.sans.edu/diary/Cyber+Security+Awareness+Month+-+Day+27+-+Active+Directory+Ports/7468