Ports

Source: https://access.redhat.com/solutions/357583 and
https://access.redhat.com/solutions/1364713

```
Source port - Destination - Protocol - Service
1024:65535 - 53 - TCP and UDP - DNS
1024:65535 - 389 - TCP and UDP - LDAP
1024:65535 - 636 - TCP - LDAPS
1024:65535 - 88 - TCP and UDP - Kerberos
1024:65535 - 464 - TCP and UDP - Kerberos change/set password (kadmin)
1024:65535 - 3268 - TCP - LDAP Global Catalog
1024:65535 - 3269 - TCP - LDAP Global Catalog SSL
1024:65535 - 123 - UDP - NTP
1024:65535 - 137 - TCP and UDP - NetBIOS
1024:65535 - 138 - TCP and UDP - NetBIOS-DGM
1024:65535 - 139 - TCP and UDP - NetBIOS-SSN
1024:65535 - 445 - TCP and UDP - Microsoft-DS
1024:65535 - 49152-65535 - TCP - Ephemerals
```

RHEL8 / OEL8 / CENTOS8

Based on instructions here:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/integrating_rhel_systems_directly_with_windows_active_directory/connecting-rhel-systems-directly-to-ad-using-samba-winbind_integrating-rhel-systems-directly-with-active-directory

We are going to setup the Linux server to use winbind for Active Directory authentication. See link from Red Hat above for more detail.

1. Allow for all AD cryptographic subpolicies
    a. 8.3 and newer: sudo update-crypto-policies --set DEFAULT:AD-SUPPORT
    b. 8.2 and older: see link above
2. Install necessary packages
    a. sudo yum install realmd oddjob-mkhomedir oddjob samba-winbind-clients samba-winbind samba-common-tools samba-winbind-krb5-locator
3. Join to Active Directory, specifying necessary user and Active Directory OU
    a. sudo realm join --membership-software=samba --client-software=winbind id-domain.mycom.com --user=hsimpson-admin@id-domain.mycom.com --

computer-ou="OU=Servers,OU=Enterprise Support,DC=id-domain,DC=mycom,DC=com"

4. Additional Winbind configuration
    a. Edit krb5.conf and add the following

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

Everything should be all set to login to the linux server as an AD user. To do so

ssh hsimpson@mycom.com@servername.mycom.com

Or

ssh ID-DOMAIN\\hsimpson@servername.mycom.com

If you don't want to use the @mycom.com or ID-DOMAIN\\, edit your /etc/samba/smb.conf and change

"winbind use default domain = no" to "winbind use default domain = yes"

RHEL7 / OEL7 / CENTOS7

Based on instructions here:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/integrating_rhel_systems_directly_with_windows_active_directory/connecting-rhel-systems-directly-to-ad-using-samba-winbind_integrating-rhel-systems-directly-with-active-directory

We are going to setup the Linux server to use winbind for Active Directory authentication. See link from Red Hat above for more detail.

1. Install necessary packages
    a. sudo yum install realmd oddjob-mkhomedir oddjob samba-winbind-clients samba-winbind samba-common-tools samba-winbind-krb5-locator
2. Join to Active Directory, specifying necessary user and Active Directory OU
    a. sudo realm join --membership-software=samba --client-software=winbind id-domain.mycom.com --user=hsimpson-admin@id-domain.mycom.com --computer-ou="OU=Servers,OU=Enterprise Support,DC=id-domain,DC=mycom,DC=com"
3. Additional Winbind configuration

a. Edit krb5.conf and add the following

```
[plugins]
  localauth = {
    module = winbind:/usr/lib64/samba/krb5/winbind_krb5_localauth.so
    enable_only = winbind
  }
```

Everything should be all set to login to the linux server as an AD user. To do so

ssh hsimpson@mycom.com@servername.mycom.com

Or

ssh ID-DOMAIN\\hsimpson@servername.mycom.com

NOTE:

If you don't want to use the @mycom.com or ID-DOMAIN\\, edit your /etc/samba/smb.conf and change

"winbind use default domain = no" to "winbind use default domain = yes"

Reboot may be required for change to take effect.

Restricting Access

Source: https://www.systutorials.com/docs/linux/man/8-realm/

- Deny all logins by default
  Realm deny --all
- Allow a specific Active Directory user
  Realm permit user@id-domain.mycom.com
- Allow a specific Active Directory group
  Realm permit --groups "example group with space in name@id-domain.mycom.com"

Linux File Permissions

Source: setfacl(1): set file access control lists - Linux man page (die.net)

If a user connects to the server via SSH, they will login with their Active Directory username and password (e.g. ssh ID-DOMAIN\\hsimpson@servername.mycom.com or ssh hsimpson@servername.mycom.com)

Once connected, files and folders will be owned by that user and the group “domain users”. “Domain users” is the default group for all Active Directory users

-rw-r--r--. 1 hsimpson domain users 0 Oct 25 10:06 somefile

If you wanted to create a folder on that server that will be shared, note users by default, when creating or SFTP’ing files, will all have the file user ownership be the active directory username (e.g. hsimpson) and file group ownership will be “domain users”

To give a specific Active Directory security group or user additional permissions, you can use setfacl to set default permissions on all files created in a folder

- E.g. Give group “domain admins” write/read/execute permissions by default on all files in the folder /somefolder

    setfacl -m d:g:"domain admins":rwx /somefolder
- E.g. Recursively give group OuAdmins-ent write/read permissions by default on all files in the folder /somefolder

    setfacl -R -m d:g:ouadmins-ent:rw /somefolder
- E.g. Recursively give user hsimpson write/read/execute permissions by default on all files in the folder /somefolder

    setfacl -R -m d:hsimpson:rwx /somefolder

To see these additional permissions, you will need to run the getfacl command. Note files will still be owned by the AD username of the user and the AD group “domain users”, but these additional permissions can be granted through setfacl

getfacl /somefolder

```
default:user::rwx
default:user:hsimpson:rwx
default:group::r-x
default:group:domain\040admins:rwx
default:group:ouadmins-ent:rw-
default:mask::rwx
default:other::r-x
```