SwiftStack

SwiftStack Gateway

Active Directory Integration

Summary

There are two main ways of integrating the SwiftStack Gateway with Microsoft Active Directory authentication:

- RID, using winbind
- LDAP

For most implementations using the RID method will typically work best, as it should work across all versions of Windows Server and Active Directory. For older versions of Windows, before Windows 2012 R2, and in cases where AD is also integrated into standard LDAP, it's also possible to use LDAP authentication.

The following sections assume that you've already set up and configured a basic functioning gateway and created a CIFS/SMB share. If you haven't done so, please go ahead and install, claim and configure a gateway before proceeding with the Active Directory integration steps below.

Prerequisites

SELinux

SELinux is currently not supported on the SwiftStack Gateway and therefore needs to be turned off. Red Hat and CentOS both have SELinux turned on and set to 'enforce' by default. To check the status of SELinux on your Gateway node, you can run:

```
$ sestatus
```

To turn SELinux off, you can edit the file `/etc/selinux/config` and replace 'enforce' with 'disabled'. For the change to take effect, you need to reboot your Gateway.

Active Directory with RID (winbind)

The SwiftStack Gateway can use Samba and winbind to query Windows RID accounts. This is the preferred way of integrating the SwiftStack Gateway with an Active Directory environment. For the integration to work, the Gateway needs to be joined to the Windows domain using an account belonging to the Windows Administrators group on the domain.

Gateway AD Domain Configuration

Before joining the Gateway to the domain you first need to configure the Active Directory settings in the SwiftStack Controller web UI. Go to the **Manage** page for the Gateway. On the left menu, click on the **Auth** tab. Click on the 'CIFS' (Active Directory) section to reveal the settings available. Fill out the FQDN or IP address of your primarily AD server. Some older versions of Windows may be case sensitive when it comes to the Windows domain name, so be sure to put in your domain name correctly.

Once you've filled out the correct settings for your domain, click on 'Submit' at the bottom of the page. Finally, after submitting the changes, you also need to push the AD configuration to the Gateway for the changes to take effect.

Joining The Gateway To The Domain

After the configuration push has completed, you must join the Gateway server to the domain. Joining the domain from the Gateway must currently be done from the command line. To join the Gateway to the domain run the following command:

```
$ sudo ad_join -r <ad-server-fqdn> -d <username> -p <password>
```

Testing That Everything Works

When the Gateway has been successfully joined to the domain, everything should work. You can test that the Gateway can indeed see accounts and groups on the domain and verify that it can authenticate properly. Except for simply testing file share access from a Windows account on the domain, you might want to run a set of diagnostics command on the Gateway to ensure it can see accounts and groups on the Windows domain:

Query domain users:

```
$ wbinfo -u
```

Query domain groups:

```
$ wbinfo -g
```

Also make sure the Gateway can authenticate users on the AD domain:

```
$ getent passwd
```

If all the above works properly, move on to functionally test that clients can see and interact with the Windows (SMB/CIFS) shares you've created on the Gateway.

Gateway CIFS Settings with RID

Below are examples from the **CIFS settings** page required to use Windows RID authentication with the SwiftStack Gateway.

Setting	Value
CIFS workgroup	DOMAIN
CIFS case sensitive	<as needed>
AD enabled	Checked
CIFS realm	DOMAIN.COM
Kerberos admin server	IP or FQDN
CIFS browser announce	0.0.0.0 (default)
CIFS id mapping	rid
CIFS id range min	-1 (default)
CIFS id range max	-1 (default)

Active Directory with LDAP

Microsoft's Active Directory is based on a Microsoft version of LDAP, and thus, it's possible to integrate the SwiftStack Gateway using LDAP too. However, using Active Directory LDAP integration requires that 'ID Management for Unix' (IDmU) tools to be installed on the Active Directory server.

IDmU has been deprecated in Windows 2012 R2 and it is therefore not recommended to install IDmU on Windows 2012 R2 (or newer). Consequently, if you are integrating with a Windows 2012 R2 based domain controller, you should use the "Active Directory with RID (winbind)" section above.

Gateway CIFS Settings with LDAP

Below are examples of the settings required to use LDAP authentication with the SwiftStack Gateway. Note that if using AD/LDAP integration, it is also required to configure the LDAP schema on the **LDAP settings** page.

CIFS Setting	Value
CIFS workgroup	DOMAIN
CIFS case sensitive	<as needed>
AD enabled	Checked
CIFS realm	DOMAIN.COM
Kerberos admin server	IP or FQDN
CIFS browser announce	0.0.0.0 (default)
CIFS id mapping	ldap
CIFS id range min	-1 (default)
CIFS id range max	-1 (default)

Gateway LDAP Settings

The following LDAP settings are examples of an LDAP schema for AD/LDAP integration with the SwiftStack Gateway. Of course, the examples below might need to be adjusted for your LDAP environment. If uncertain, please consult your organization's LDAP administrator.

LDAP Setting	Value
LDAP enabled	Checked
LDAP server list	<FQDN or IP of LDAP servers>
LDAP server port	389
LDAP version	3 (default)
LDAP base DN	<your LDAP base DN>
LDAP bind DN	<your LDAP bind DN>
LDAP bind password	<your LDAP bind password>
LDAP scope	subtree (default)
LDAP timeout	5
LDAP bind timeout	5
LDAP referrals	Checked (default)
LDAP group lookups	Unchecked (default)

Troubleshooting

`wbinfo` shows AD users/groups, but `getent` doesn't

While winbind is capable of talking to Active Directory to get AD user and group information, the actual gateway relies on its internal Name Services to look up users and groups. Information from winbind is fed into the Name Services via a special winbind 'libnss'. On Ubuntu, this library is provided in a separate package called 'libnss-winbind'. If this package is not installed, username/group resolution will not work.

To remedy, manually install this package with the command:

```
$ sudo apt-get install libnss-winbind
```

On CentOS/RHEL, this library is included with the winbind packages, and does not need to be installed separately.