LibcloudSSL

Background

Python does not perform SSL certificate name verification out of the box.

To address this, we've introduced the **libcloud.security** module with tunable parameters.

Accordingly, the LibcloudHTTPSConnection objects load settings from this module and performs hostname checks against the `commonName` and `subject AltName` DNS entries.

Requirements

At time of writing, this change pushes the requirement of the `ssl` PyPI *package* for 2.5+, as 2.6+ contains the built-in `ssl` *module*.

Usage

Disabling SSL Certificate Check

Setting **VERIFY_SSL_CERT** to False is currently the default behavior of 0.4.1-dev. This will likely change in future versions.

```
import libcloud.security
libcloud.security.VERIFY_SSL_CERT = False
```

When this value is false, it emits a UserWarning:

{{{#!bash libcloud/httplib_ssl.py:55: UserWarning: SSL certificate verification is disabled, this can pose a security risk. For more information how to enable the SSL certificate verification, please visit the libcloud documentation.
warnings.warn(libcloud.security.VERIFY_SSL_DISABLED_MSG)
}}}

Enabling SSL Certificate Check

```
import libcloud.security
libcloud.security.VERIFY_SSL_CERT = True

# optionally, add to CA_CERTS_PATH
libcloud.security.CA_CERTS_PATH.append("/path/to/your/cacerts.txt")
```

CA_CERTS_PATH contains common paths to CA bundle installations on the following platforms:

- **openssl** on CentOS/Fedora
- **ca-certificates** on Debian/Ubuntu/Arch/Gentoo
- **ca_root_nss** on FreeBSD
- **curl-ca-bundle** on Mac OS X

Example Failure Scenarios

Missing Valid Certificate Authority

When a valid CA cannot be found in **CA_CERTS_PATH**, one may see the following stacktrace:

{{{#!bash libcloud/httplib_ssl.py:75: UserWarning: Warning: No CA Certificates were found in CA_CERTS_PATH. Toggling VERIFY_SSL_CERT to False.
warnings.warn(libcloud.security.CA_CERTS_UNAVAILABLE_MSG)
}}}

Certificate Hostname Mismatch Failure

When the hostname does not match the certificate, an SSLError exception is raised.

To manually test, one can edit the HOSTS file to point a Provider API hostname to another SSL-enabled site, and the result should be:

```
{{{#!bash
File "libcloud/httplib_ssl.py", line 99, in connect
raise ssl.SSLError('Failed to verify hostname') ssl.SSLError: Failed to verify hostname
}}}
```

Miscellaneous

OS X: Batteries Not Included

The current issue with OS X root certificates is that they're stored in the Keychain format, unlike the standard PEM format available on other *nix platforms.

Acquiring CA Certificates

If the above packages are unavailable to you, and you don't wish to roll your own, the makers of cURL provides an excellent resource, generated from Mozilla: http://curl.haxx.se/docs/caextract.html

Feedback

Any feedback, please send to the mailing list at libcloud@incubator.apache.org or the JIRA at https://issues.apache.org/jira/browse/LIBCLOUD.