Upgrade to v5.12.1 results in an "untrusted" SSL connection when a trusted certificate was used

Symptom

After upgrading to v5.12.1, the web browser reports an untrusted SSL connection when previously a trusted SSL certificate was used

Cause

The Server Backup Manager allows administrators to provide their own trusted or self-signed SSL certificate. Early versions of the documentation specified importing the SSL certificate using an alias of "importkey". This documentation was incorrect. The correct certificate alias is "cdp" and usage of the "importkey" alias only worked due to undocumented behavior in the Java SSL keystore programming library.

The 5.12.1 release corrects an issue with R1Soft's handling of the default self-signed certificate added during product installation. The 5.12.1 release also resolves the issue of overwriting the Java keystore during product upgrades.

These improvement to SSL certificate management require the use of the correct certificate alias, rather than relying upon undocumented behavior in the Java library.

Resolution

SSL certificates should be imported into the Java keystore using an alias of "cdp". This applies to all versions of the product. Certificate installation is documented here: Run Server Backup Manager over SSL (HTTPS)

In version 5.12.1, the existence of a "cdp" aliased certificate is verified and if not found a self-signed SSL certificate is automatically installed. Any existing certificates will remain in the keystore.

If a trusted certificate exists with an alias of "importkey" or another alias, then the alias can be changed with the following command:

```
# keytool -changealias -keystore keystore -alias importkey -destalias cdp
```

If a self-signed SSL certificate already exists with an alias of "cdp", then the certificate may be removed with the "-delete" keytool command or renamed per the example above.

The Java keytool utility is documented here: Java keytool

NOTE: The Java certificate keystore can be modified to use the "cdp" alias with any version of the Server Backup Manager. Updated the keystore prior to upgrading to 5.12.1 will prevent any unexpected behavior for SSL connections.

NOTE: Following any alteration of the SSL keystore, the Server Backup Manager must be restarted in order for the changes to take effect.