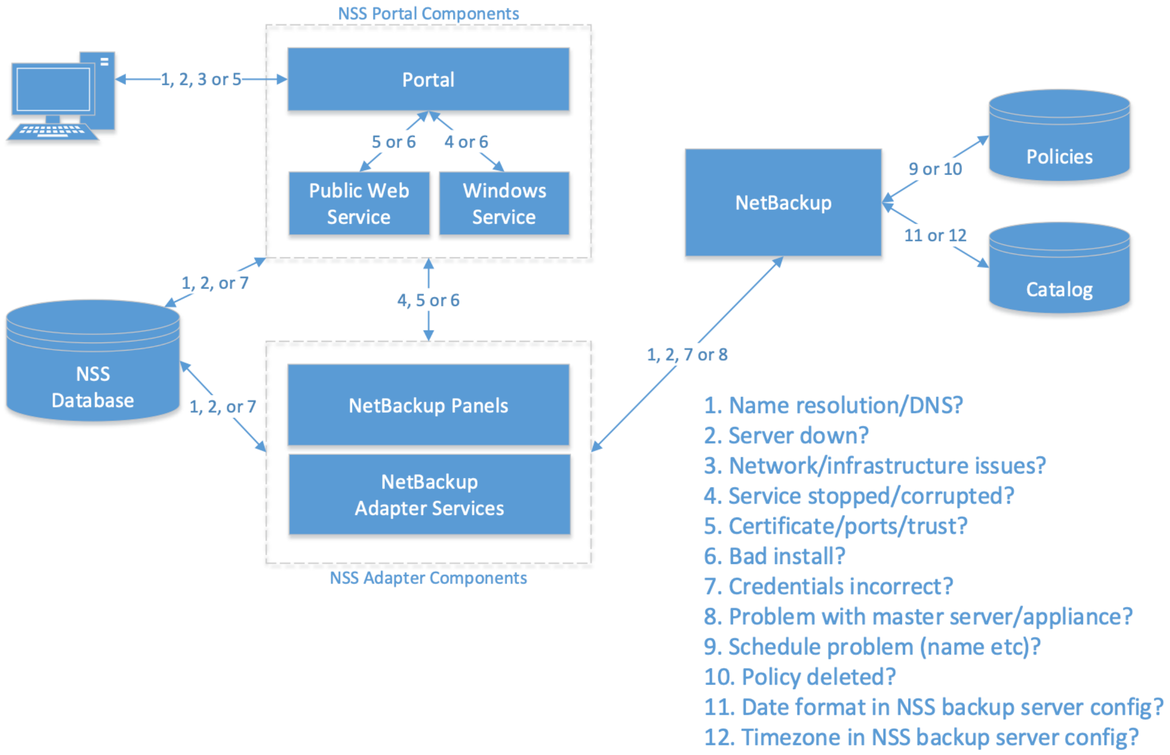
NSS Basic Troubleshooting



1. Name resolution/DNS?
2. Server down?
3. Network/infrastructure issues?
4. Service stopped/corrupted?
5. Certificate/ports/trust?
6. Bad install?
7. Credentials incorrect?
8. Problem with master server/appliance?
9. Schedule problem (name etc)?
10. Policy deleted?
11. Date format in NSS backup server config?
12. Timezone in NSS backup server config?

NSS Basic Troubleshooting Notes

1. Test if the hostname can be resolved. If not, fix resolution via DNS or host file.

   Errors relating to name resolution tend to be along the lines of ‘server not found’, ‘host not found’ or in the case of HTTP errors, 404 – Not found. A ping to the hostname is likely to time out, while a ping to the expected IP address will succeed.

2. If there is a valid host file or DNS entry for the hostname, is the server down?

   Same errors to item 1 above, but in this case, it is not related to missing name mapping. Both a ping to the hostname *and* a ping to the expected IP address will timeout and fail.

3. Are connection issues related to network/server latency, additional network layers?

   Errors in this case may be similar to items 1 and 2 above, but related operations may sometimes succeed without error. You may receive timeout errors. Security software may interfere with traffic and cause unexpected behaviour – you can check associated policies with your security team. Where a client browser is being used, are requests routing through a proxy server? If so, is it operational and contactable? If NSS is load balanced/clustered, are all nodes operating as expected?

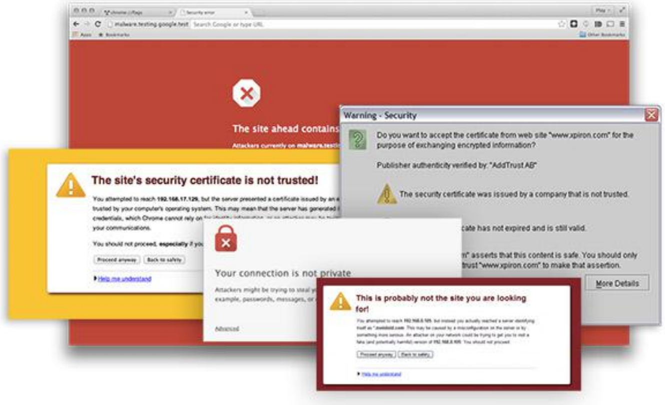
4. The Windows service runs scheduled tasks and fulfilment workflows in NSS. It is essential for NSS to fully function. If synchronisation or workflows do not proceed, ensure the Windows service is running.

The Configuration Check page will show whether the service is running or not. Alternatively check the Windows Services applet. Errors may be absent from NSS, but scheduled tasks and workflow stages will not proceed. On the Monitoring tab, the System Update which runs every minute may show it last ran more than a minute ago. Restart the Windows service.

5. As NSS is a web application. Certificates are required for HTTPS communication. Mismatches between host names and certificates and expired certificates can cause issues where NSS will not display pages. Ensure certificate is valid. Also ensure ports being used are correct and, if domain trust is required between NSS web server and the client browser, they have been set up correctly by your network team.

   Typical errors include: "The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel."

   If using a self-signed certificate, you may receive a warning:



The site ahead contains

Warning - Security

Do you want to accept the certificate from web site "www.xpiron.com" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "AddTrust AB"

The security certificate was issued by a company that is not trusted.

cate has not expired and is still valid.

n" asserts that this content is safe. You should only trust "www.xpiron.com" to make that assertion.

The site's security certificate is not trusted!

You should not proceed, especially if you

Your connection is not private

This is probably not the site you are looking for!

   This is normal, as you are using a certificate not recognized by the browser (as it is not registered with a cert authority). Some browsers allow you to add an exception so you don't see these warnings in future.

6. If components are missing or referenced incorrectly, NSS may not behave as expected. Were any errors experienced during install? Were all install steps followed correctly?

   This is unlikely if the system has been operating as expected for a while. If, however, the system has never operated as expected and other troubleshooting steps have been followed with no success, you may need to reinstall the system.

7. Where NSS web components communicate with an external application, credentials will be used to authenticate. If NSS cannot communicate with the external application, are the credentials correctly configured in the appropriate NSS configuration? In the case of database credentials, has the password of either database changed since installation?

   Errors where credentials are incorrect usually state that is the case in some way: e.g. 'Login failed', 'Cannot login', 'Invalid credentials' etc. The equivalent HTTP error is 401: Unauthorized.

8. Master server/appliance problems

   Sometimes it may be the case that the NetBackup Master Server or Appliance does not meet the pre-requisites for NSS or may be not be configured for compatibility (NSS requires sudo when sending CLI commands to Unix masters, for example). Ensure the master server/appliance meets the pre-requisites for NSS and any incompatibility is resolved.

   A technote on some issues with particular versions of master server/appliance is available here:

9. Schedule problem

   Some functionality in NSS requires that a pre-existing schedule exists on a policy to be updated. This might be the 'Default' schedule on a backup now policy or a schedule name defined in an NSS Protection Level.

   Typical errors: 'Entity not found' during a backup now request, **** during a Protection Level request.

10. Policy deleted?

    NSS uses deactivated, pre-configured 'template' policies which it copies to create ongoing, active scheduled policies. NSS periodically checks these active policies for client membership and updates the protection status of assets. This means NSS expects specific policies to exist on the master server. However, it is possible for any of these expected policies to be deleted manually in error.
    Where a template policy has been deleted, you can expect an error such as: *** or you'll notice in the Protection area of NSS that Protection Types may be shaded, indicating missing template (you can hover over the ? to find out what the issue is).

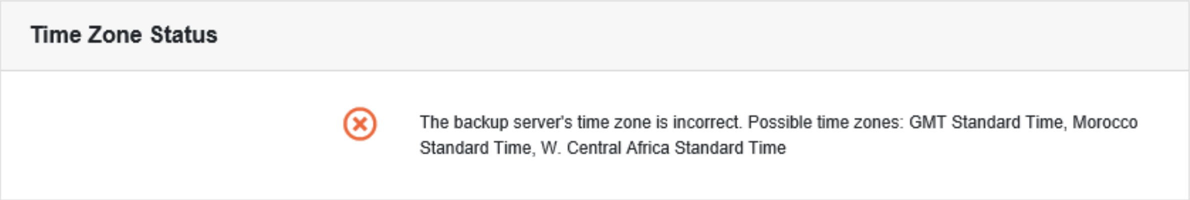
    If there is a missing scheduled policy, the nightly sync will assume assets are no longer protected when the system next syncs with the master server as when NSS checks policies for client membership, the policies will no longer exist. **Protection status will be affected**.

    Active and ongoing NSS scheduled policies should never be deleted manually, unless advised by Veritas.

    If you find that expected protection has been lost in NSS, investigate whether the associated policies exist.

11. NSS by default uses the US date format when issuing commands to the master server. Date format errors may indicate the date format configured on Backup Server is not correct. This is rare. Most masters use US date format as standard.

    This mismatch is picked up by the connectivity check in NSS:



Time Zone Status

The backup server's time zone is incorrect. Possible time zones: GMT Standard Time, Morocco Standard Time, W. Central Africa Standard Time

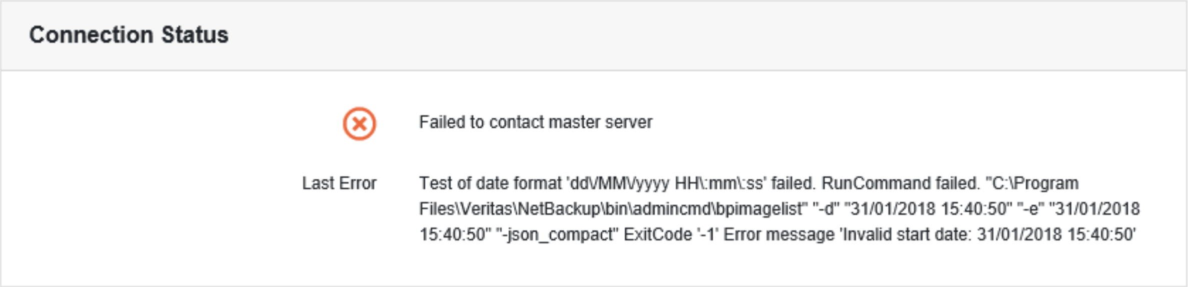
When performing a restore from a backup image, resources would not be found. E.g. a file restore would show no files in the browse dialog.

Always check connectivity to backup servers if experiencing any operational issues in NSS.

12. NSS stores times in UTC format and offsets them when sending commands to a master server depending on its timezone. If NSS cannot find expected images for a specific timeframe, this may indicate an issue with the timezone configured on the Backup Server in NSS.

    The timezone must match that which the master server itself is set to.

    A connectivity check reveals the problem:



Connection Status

Failed to contact master server

Last Error

```
Test of date format 'dd\/MM\/yyyy HH\:mm\:ss' failed. RunCommand failed. "C:\Program Files\Veritas\NetBackup\bin\admincmd\bpimagelist" "-d" "31/01/2018 15:40:50" "-e" "31/01/2018 15:40:50" "-json_compact" ExitCode '-1' Error message 'Invalid start date: 31/01/2018 15:40:50'
```

Performing a restore operation would show an ‘invalid start date’ error.

Always check connectivity to backup servers if experiencing any operational issues in NSS.