Troubleshooting Bit9 Agent Connectivity

Parity Version 6 and 7

Overview

This brief gives specific information on the basics of troubleshooting the Bit9 Agent's connectivity to the Bit9 Server. We cover basic tests and diagnostics gather, symptom sets and possible solutions.

Theory of Operation

The Bit9 Agent uses standard and compliant HTTP over SSL to communication with the Bit9 Server. It communicates this way on both TCP port 443 and TCP port 41002.

This means that anything on the network, between the Bit9 Server and a given Bit9 Agent, that can affect these protocols, has the potential to disrupt agent/server communication. For example firewalls and web proxies could cause a problem.

The Bit9 Agent uses the Microsoft Windows "WinHTTP" library for all communications. This means that configuration settings on the local computer, that effect the operation of WinHTTP, have the potential to disrupt agent/server communication. For example, proxy settings for Microsoft Internet Explorer could cause a problem. Note that the Bit9 Agent runs in the "system" context, so per-user settings may not cause issue, but per-system settings will.

The Bit9 Agent itself may also be stopped, crashed, or hung, which would of course prevent it from communicating with the Bit9 Server.

It is beyond the scope of this document to describe how to resolve all possible problems that might cause a connectivity issue. Certainly, it is beyond the scope of this document to describe how to troubleshoot problems with local machine configuration. However, this document will at least allow you to generate a clear description of the problem, and to create a good hypothesis about the cause, so that you may engage the correct resources.

Bit9 Agent "Status" Command

Every computer that has the Bit9 Agent installed has a "status" command that can be used to gain information about the agent's connectivity.

Running the Command

1. Open a command prompt.
2. On a 32-bit system, run the command "cd c:\program files\bit9\parity agent".
    a. On a 64-bit system, run the command "cd c:\program files (x86)\bit9\parity agent
    b. Note that this command assumes the default install location for the Bit9 Agent. If you believe that you are using an alternate install location, contact your Bit9 expert to find out what that location is.
3. Run the command "dascli status" and examine the output.

If the command returns no output, or if it returns a message claiming that the "agent or service could not be contacted," this means that the Bit9 Agent has been stopped, is not running, or has crashed or experienced a hang. A section later in this document describes how to begin to troubleshoot that issue.

Sample Output

```
Version Information
    CLI:        7.0.0.1639 Oct 21 2013 08:33:08
    Agent:      7.0.0.1639 Oct 21 2013 08:31:06
    Kernel:     7.0.0.1639 Oct 21 2013 08:46:41
    Server:     7.0.0.1639 Oct 21 2013 08:34:17

Enforcement Information
    Current:            Medium (Prompt Unapproved)
    Connected:          Medium (Prompt Unapproved)
    Disconnected:       Medium (Prompt Unapproved)

Cache Information
    Cache State:        Initialized Priority[1] Complete[100%]
    Cache Check:        Not running Type[0] Options[None]
    Global Approvals:   310054 (290787 Active)
    Global Bans:        20 (20 Active)
    Unique Files:       47213
    Total Objects:      71968 Files, 4770 Events, 28646 File Report
    Under Analysis:     0 Started, 0 Ready, 83 Initiated
    Analyzed:           11739
    Database Queue:     R:0, W:0, X:0

Server Information
    Server:             stratocaster.bit9.com:41002
    Policy:             Customer Facing Teams (17-00000005)
    Config List:        392375
    Register Count:     2 (Last 11/7/2013 9:05:55 AM)
    Poll Count:         232 (Last 11/7/2013 10:42:29 AM)
    File Uploads:       0
    Unsent Queue:       2 Events, 0 File Reports
    Sent Queue:         380941-409585
    Prioritized:        No

Client Information
    Client:             workxp001.bit9.com (AD1\WORKXP001$)
    MAC Address:        00:26:77:45:AA:12
    Connection:         Connected (Ok)
    Session:            Active
    Certificates:       Verify, Allow Expired
    Debug Level:        0
    Kernel Level:       2/007FFFFF
    Parity Dumps:       0 (Never)
    Windows Dumps:      0 system (Never); 0 mini (Never)
    Network Trace:      Disabled
    Tamper Protection:  Enabled
    Windows Update:     Inactive
    SSL Mode:           Strong (Validate CAs, Validate CNs)
    Upgraded:           Unavailable
    Health Status:      Healthy
```

Analyzing the Output

In the "Server Information" section, the field "Server" shows the name of the Bit9 Server.

The Bit9 Agent uses this name and this name only to contact the Bit9 Server. This name must "be resolvable and resolve correctly" on the workstation, to the appropriate IP address of the Bit9 Server, or proxy that will handle the connection. Any proxies managing the connection must also be able to resolve this name appropriately. This name must also be present as the "common name (CN)" or as a "subject alternate (SA)" in the SSL certificate on the Bit9 Server.

In the "Client Information" section the field "Connection" shows information about the status of the agent's connection to the server.

"Connected (OK)" suggests that the agent is communicating properly with the server.

However, you may see an OK status at the agent, but your Bit9 Server administrator may tell you that the agent shows as disconnected in the Bit9 Administration Console. This indicates one of two possible problems.

First, it is possible that your agent is connecting and disconnecting so rapidly that the server does not see the connection as "persistent." You may wish to run the status command every few seconds over the course of a few minutes, to see if the status changes back and forth between "connected" and "disconnected." If so, it could be happening because your network connection is unstable or your machine is experience severe performance problems. It could also be happening because there is a problem with the Bit9 Agent itself, or the Bit9 Server. Once you classify the problem this way, engage experts to help you further troubleshoot.

Second, if you agent appears to remain continuously connected, as evidenced by running the status command repeatedly as instructed above, this likely indicates a problem with the Bit9 Server. Specifically, it means that the Bit9 Server is having a problem adding the connection status to its database, and therefore reporting on it in the console. Once you classify the problem this way, engage the Bit9 Server administrator to further troubleshoot.

"Disconnected" means that the agent is legitimately disconnected from the server.

This means the agent assumes there can be no connection to the server, perhaps because the server's name is "not resolving" in DNS, you need to be on the VPN in order to access the server, or a firewall is blocking basic connectivity. Engage your network experts in order to troubleshoot.

“Connect” or “disconnected” status may also show an HTTP error code.

HTTP Error 0 most likely means problems with the SSL connection. For example, maybe a proxy is terminating the SSL in an invalid way. Or perhaps the server name that the Bit9 Agent uses is not present in the SSL certificate on the server, or maybe the server certificate has expired. Engage your SSL experts in order to further troubleshoot.

HTTP Error 401 means “access denied.” It is possible that certain permissions on the Bit9 Server were accidently changed and are now preventing access, and so you may want to contact the Bit9 Server administrator. However, the most common reason this error occurs is because a proxy stands between agent and server, and is not correctly routing the request. Note that some proxies require “authentication.” The Bit9 Agent runs in the context of “system,” not the end users, and this machine change the nature of, or make impossible, the agent’s use of the proxy.

HTTP Error 404 means “not found.” It is possible that the Bit9 Server application has been uninstalled, or that the application has been moved from this server to a different one. However, the most common reason this error occurs is because a proxy stands between agent and server, and is not correctly routing the request.

HTTP Error 500 could indicate a problem with the Bit9 Server, and so you should contact the server’s administrator. Sometimes this error occurs because a proxy stands between agent and server, and is not correctly routing the request.

Using Internet Explorer to Test Connectivity

You can use Microsoft Internet Explorer to test connectivity to the Bit9 Server.

Note that the Bit9 Agent runs in the context of "system," whereas when you test with Internet Explorer (IE), you will be testing in the context of your user logon.

If your tests with IE are successful, but the agent still appears to have connectivity problems at the network or SSL level, that likely means that your IE proxy settings for your account are correct for your environment, but the "system" settings for the proxy are not. Your workstation's system administrator needs to set the proxy for "system" correctly.

If your tests with IE are successful, but the agent still appears to have connectivity problems at the network or SSL level, it may indicate that the proxy is "authenticating," and that "system" cannot authenticate to it. Contact your proxy administrator for more details.

Running the Test

1. You will need the server name from the status command above.
2. First, point your browser at https://server.hostname.com:41002, where "server.hostname.com" is your server's name.
3. Wait for the connection to succeed or fail, then observe and record the results.
4. Then, point your browser at https://server.hostname.com:443, where "server.hostname.com" is your server's name.
5. Again, wait for the connection to succeed or fail, then observe and record the results.

Ports 41002 and 443

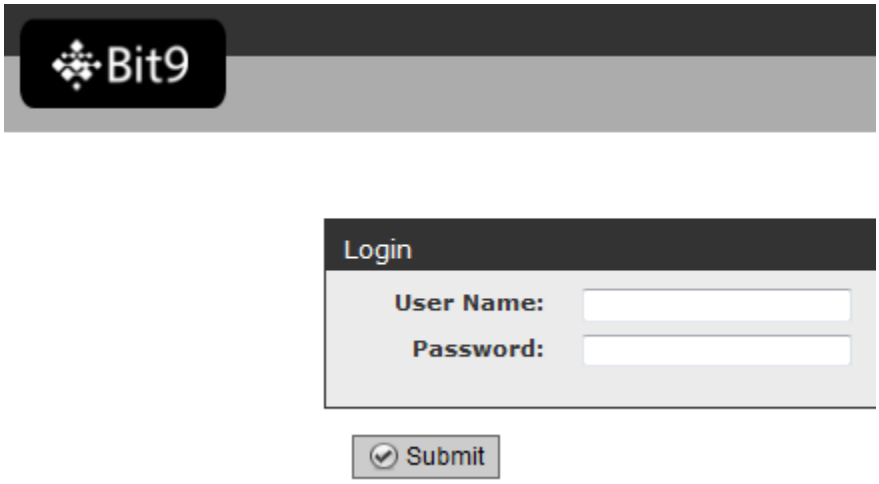
We have you run the test twice on two different "ports," because the agent uses two different channels to communicate with the server, and uses each one for different things.

Most of the agent traffic goes over port 41002. If this connection is failing, the agent will show so in the connection status, and will not be able to communicate with the server at all.

Certain diagnostic and upgrade functions go over port 443. If port 41002 works OK but port 443 does not, the agent will show a connected status as OK, and will get most information from the server. However, certain specific functions will fail when you try to trigger them, such as uploading diagnostics or pushing an agent upgrade from the console.

Results in the Browser

A successful test on port 443 shows the Bit9 Administration Console logon page:

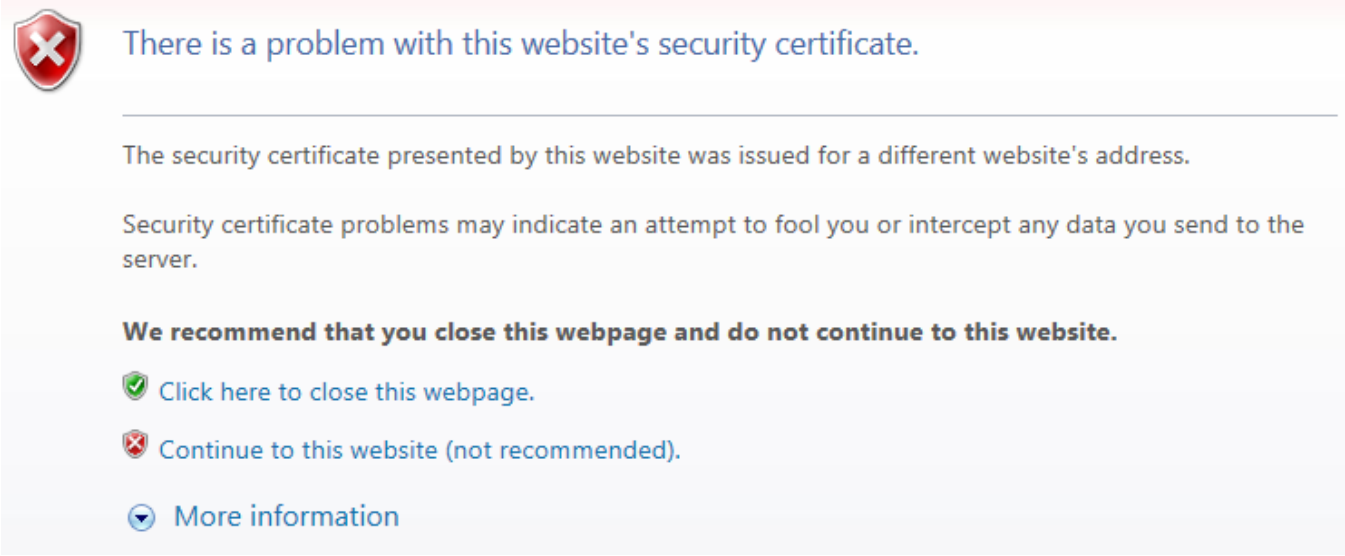


A successful test on port 41002 is harder to demonstrate. The browser will appear to process the request for a very long time, and then it will timeout. Unfortunately, this same behavior can also be indicative of network firewall problems.

One thing you can try is use the IP address of the Bit9 Server instead of the hostname. You may need to contact your Bit9 Administrator or network administrator for this. If you use the IP address instead of the hostname, and if a connection is successful, you should get an SSL certificate error like what is mentioned below.

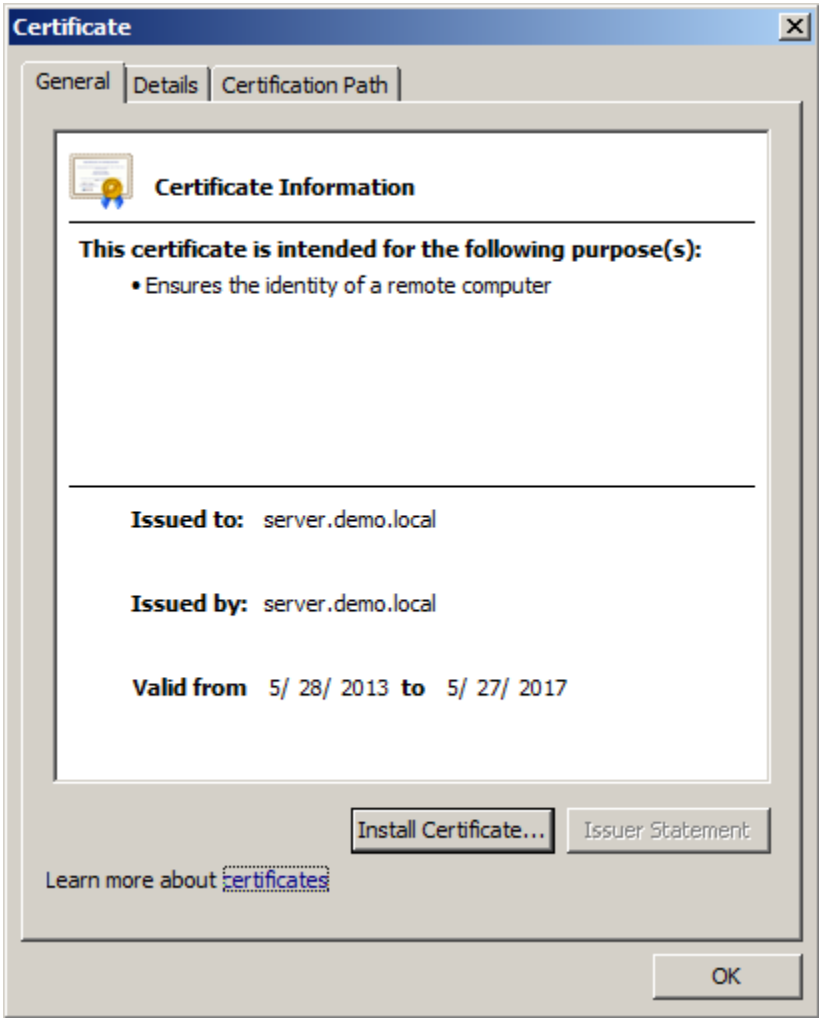
Also, if "telnet" is installed on your workstations, you can try to use it to connect to the Bit9 Server on port 41002. Open a command prompt and type "telnet hostname 41002" where "hostname" is replaced with the name or IP address of the Bit9 Server. If a connection is successful, the command prompt window will go blank, except for a blinking cursor. You can press "Control-C" to quit the telnet session. This test may not work if you need to use a web proxy to access the Bit9 Server.

Even when you use the Bit9 Server's hostname, you may encounter an SSL certificate error:



You must take some additional action to better understand the nature of this error. First, click the "Continue to his web site (not recommended)" link. Then, near the top of your browser in the URL bar, click the "Certificate Error" button:

Then, in the dialog box that pops up, click the “View Certificates” link. You should receive another dialog box that shows you details of the certificate:



Today’s date must be within the range specified by “Valid from.” And the hostname that the Bit9 Agent uses to connect to the Bit9 Server, the one you learned about from the “dascli status” command, must match exactly the name in the “Issued to” field. If either of these is not correct, there is something wrong with the SSL certificate on the Bit9 Server, or with the SSL termination on your web proxy, and you will need to contact the appropriate administrator.

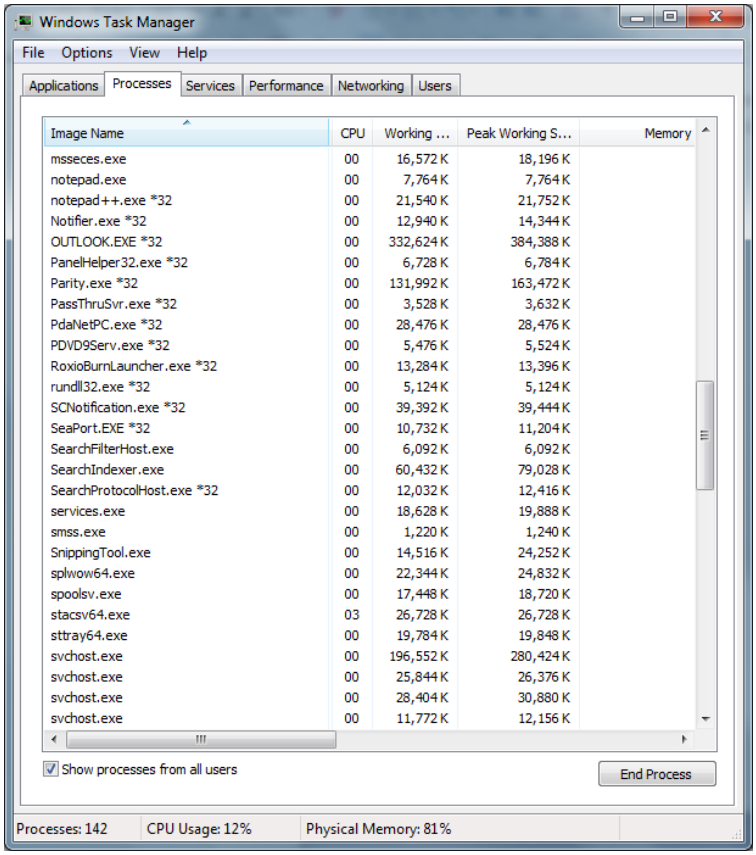
Diagnosing Agent Problems

In the section on using “dascli” we mentioned that the Bit9 Agent might be stopped, crashed, or hung. Diagnosing the full root cause of this issue may be complex and will likely require Bit9 experts. However, there are some basic things you can do to classify the issue.

Is the Bit9 Agent running?

The Bit9 Agent may not be running, and you can check to see if this is so. You may need system administration privileges to conduct these steps.

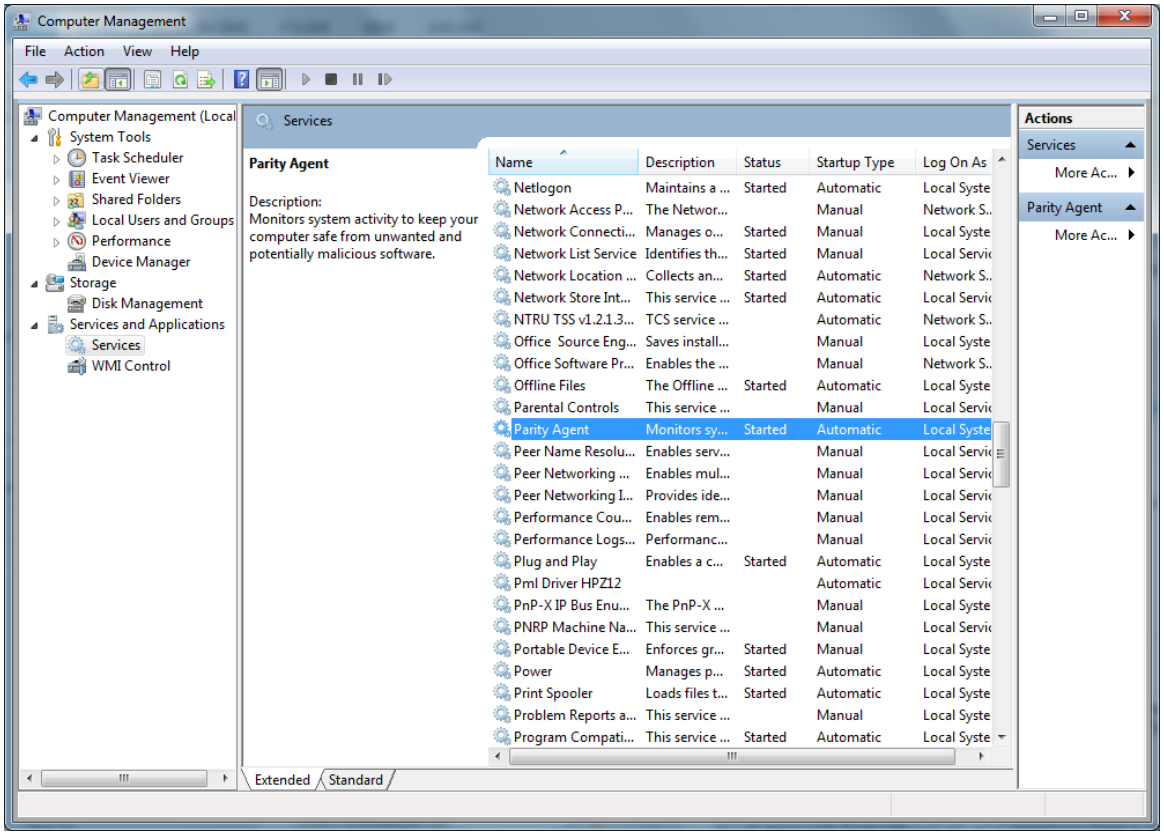
1. Right-click on the Windows menu bar at the bottom of your desktop, and choose “Start Task Manager.”
2. Go to the “Processes” tab. Also, click the “Show Processes From All Users” button at lower left.
3. Click the “Image Name” column header to sort the processes in alphabetical order.
4. Do you see the process called “parity.exe” in the list?



Can you start the Bit9 Agent?

If the Bit9 Agent is not running, you may be able to start it again. Also, you may be able to determine if it is able to start automatically. You may need system administration privileges to conduct these steps.

1. Click the Windows logo "Start" button at the lower left of your screen, then right-click on "Computer" and choose "Manage."
2. If you are prompted to run the application with privileges, click "OK."
3. Expand the "Services & Applications" node at the bottom of the list on the left, then click the "Services" node.
4. In the list, look for the item called "Parity Agent."
5. Right-click on this item and choose "Start."
6. Also, look at the volume in the column labeled "Startup Type." The value for "Parity Agent" should be "Automatic."
7. You can right-click on "Parity Agent" and choose "Properties" in order to change the "Startup Type."



How permanent is the hang?

If “dascli status” reports that it cannot connect to the user agent, or if it reports no output at all, and if the “parity.exe” process is running, then the agent is hung.

Be sure to report whether “dascli status” returned an error, or if it returned no output. It may also be useful to run it several times over the course of a few minutes, to see if sometimes it works and sometimes it does not. Or you may find that it returns status correctly, but the response may take a very long time. Report any such details when you are describing the problem.