Title: Exploring DC Agent In Depth

This Webinar covers the most popular requested Knowledge Base article topic, "issues with DC Agent."

- Identification issues begin with end users being incorrectly filtered. This exhibits itself as end users being incorrectly filtered due to:
    - Missing user name.
    - Incorrect user name.
    - Duplicate user names.

Preliminary network assessments:

1. Check external influences that may be causing trouble.
    a. Network Changes.
        i. Switches, routers, firewalls, …
        ii. DC Agent required NetBIOS port 139 opened.
    b. Are Websense services installed on supported operating systems?
        i. Were any servers upgraded?
    c. Do Websense services support your Directory Service?
        i. Was your directory service upgraded?
        ii. Early Websense versions did not support Windows 2008 Active Directory.
        iii. Upgrade or apply hotfixes.
    d. Review the Deployment Guide for support details.
2. Check for available Websense hotfixes.
    a. www.MyWebsense.com.
    b. Websense services for identification are:
        i. DC Agent, Filtering Service, User Services.

Check the reporting output to see the name currently displayed:

3. Run TestLogServer utility.
    a. TestLogServer –onlyip 10.10.10.10 –file test.txt
    b. The output shows the recorded user name?

Pull user map from DC Agent:

4. ConsoleClient <IP of DC Agent> 30601
    a. Select menu options:
        i. PrintSelf
        ii. Dump to Local File
        iii. Level=3
        iv. <filename>.txt (Enter any appropriate file name.)
        v. XID User Map
    b. Are there multiple DC Agents?
        i. TRITON –Web Security manager show all DC Agents.

c. KB Article: “Troubleshooting DC Agent with ConsoleClient”
    i. http://www.websense.com/support/article/t-kbarticle/Troubleshooting-DC-Agent-with-ConsoleClient

5. DC Polling feature.
    a. Must be enabled in TRION – Web Security
    b. DC Agent records user name/IP address pairs:
        i. For each logon session, DC Agent performs a DNS lookup to resolve the computer name to an IP address, and then stores the user name/IP address pair in its user map in local memory.
        ii. Periodically, every 10 minutes, it writes a copy of the user map to **XidDcAgent.bak** file.
    c. Initially, Filtering Service contacts DC Agent for a complete copy of the user map.
        i. Afterwards, DC Agent updates Filtering Service only for newly added user name/IP address pairs.

6. User map is blank.
    a. Is the DC Agent service running? If not, then:
        i. Reset password for logon account.
        ii. The Log On account may be locked out.
        iii. Test using a different domain Admin account as the Log On account.
        iv. Does the service start with no Log On account?
    b. Verify DC Agent can poll your domain controllers.
        i. Logon with the same account assigned to DC Agent and run the following command:
            1. **C:\>net view /domain > list.txt**
        ii. If your domains are returned, then DC Agent should also see the same data.
    c. Does **the \Websense\bin\dc_config.txt** file exist?
        i. The Domain Controller Polling feature uses this file to identify which domain controllers to monitor for user logon sessions.
        ii. **If the file does not exist (1),** then enforce DC Agent to create the file.
            1. Add **UseUserService=False** to the **\Websense\bin\transid.ini** file.
                a. By default, User Service creates the **dc_conf.txt** file.
                b. This setting tells DC Agent to create the file.
            2. Restart DC Agent service.
            3. After about 2 minutes, the **dc_config.txt** file should be created automatically.
        iii. **If file does not exist (2),** create it manually.
            1. On 2008 servers, open and run Notepad as an Administrator.
                a. Right click on Notepad and select run as administrator.
            2. Populate the **dc_config.txt** file with domain controllers, for example:

[TESTADW2K3]
AD2W2K3=on
AD1W2K3=on
[SURFTESTADW2K3]
SFAD1W2K3=off
SFAD2W2K3=off

3. The file should include all domain controllers, which end users filtered by Websense could possibly log onto.
    a. These should be set as **=on** status.
4. Domain controllers that users will not log into should be listed.
    a. These should be set as **=off** status.
    b. Set unnecessary domain controllers, in the **dc_config.txt** file, to **=off** status.
5. Consider number of DC entries set as **=on** status.
    a. Generally, the list should not exceed 10-20 domain controllers set to **=on** status.
        i. The exact number varies accordingly network bandwidth and latency.
        ii. Latency to any domain controller should be under 30 milliseconds.
    b. Install multiple DC Agents to reduce the numbers actively monitored domain controllers listed in the **dc_config.txt** list.
        i. Modify the **dc_config.txt** such that a domain controller listed as **=on** for one DC Agent is set as **=off** all other DC Agents.
    c. Install a DC Agent at any remote site with a slow link, and set it to monitor only its local domain controller.
6. Re-start DC Agent service after changing the **dc_config.txt** file.

iv. NetBIOS must be enabled for DC Agent to contact the domain controllers.
1. On Local Area Connection Properties, select Internet Protocol (TCP/IP) > Properties button > General tab > Advanced button > WINS tab > Enable NetBIOS over TCP/IP.

v. Is the **DiscoverInterval**, in the **transid.ini** file, disabled?
1. The **DiscoverInterval** value determines how often DC Agent looks for new domain controllers.
    a. By default, DC Agent checks for new domain controllers every 86400 minutes (which equals 24 hours) or upon service restart.
2. It is disabled when set to:
    a. DiscoverInterval=0
3. By default, discovery is enabled and set as follows:
    a. **DiscoverInterval=86400**

7. User names quickly disappear from the user map or not picked up consistently.
    a. Check Domain Controller Poling settings.
        i. **Query interval** default is **10 seconds**.
        ii. **User entry timeout** default is **24 hours**.
    b. DC Agent only picks up users who log into the network or request network resources.
    c. Users who lock their workstation and are not logged into the network the following day when unlocking their system.
    d. A service account is seen upon boot-up.

8. The user map is populated, but contains incorrect names or missing names.

a. From a DOS window on the end user's workstation, run the **SET L** command to see how the user logged in.
    i. Locally – must log into the network for DC Agent to pick up the user name.
    ii. Network – the domain controller shown must be listed in the **dc_config.txt** file.
b. Do the user names contain special characters?
    i. You can ignore special characters by entering **StripNonSpaceCharacters=True** in the **tranid.ini** file.
c. Service names appear in User map
    i. Names, identified in the **\Websense\bin\ignore.txt** file are "not" added to the user map.
    ii. Add service account names, appearing in the user map, to the **ignore.txt** file.
    iii. Default entries, in the **ignore.txt** file, for service accounts for English operating systems are:
        1. **local service**
        2. **network service**
    iv. For non-English operating systems, add the native language service account names. For example, the French default account names are:
        1. **service local**
        2. **service réseau**
    v. Restart DC Agent service after changing the **ignore.txt** file.
d. The Computer Polling feature (WKSPOLLING) can populate incorrect or blank user names.
    i. This feature reads the user name from the windows logon key in the registry.
        1. A domain administrator account is required.
        2. Workstation firewalls must allow DC Agent to access the registry.
    ii. This feature can be problematic.
    iii. This feature can be responsible for inserting blank user names in the user map.
    iv. Typically, we in techsupport disable the Computer Polling feature.
        1. Disable in TRITON – Web Security under User Identification.
    v. This feature is being re-engineered in v7.6, due out later this year.
        1. You will want to re-evaluate this feature after upgrading to v7.6.
e. To update or remove user names from the DC Agent user map.
    i. Re-log into the network.
    ii. Run the **NET USE %LOGONSERVER%** command.
        1. For example, type: **net use //<domain_contoller_name>**
    iii. Wait for user names to expire from the map.
        1. Default timeout value is 24 hours.
    iv. Manually clear the cached user map.
        1. **Note: This should be performed with caution in a production network.**
        2. Stop DC Agent service (XidDcAgent.exe) to clear its cache.
        3. Rename **XidDcAgent.bak** file.
            a. This file contains a hard copy, of the user map, such that when restarting user names are retained. The file is updated every 10 minutes.
        4. Start DC Agent service.
        5. Stop and restart Filtering Service.
            a. Filtering Service hold a copy of the user map in cached memory.

b. When restarting Filtering Service, it asks DC Agent for a user map update.

6. For new names to be picked up, all users must relog into the network or request a network resource.

If DC Agent's user map contains the correct user names, then pull the Filtering Service user map:

9. ConsoleClient <IP of DC Agent> 15869

a. Select menu options:
   i. PrintSelf
   ii. Dump to Local File
   iii. Level=3
   iv. <filename>.txt (Enter any appropriate file name.)
   v. XID User Map

b. KB Article: "Troubleshooting DC Agent with ConsoleClient"
   i. http://www.websense.com/support/article/t-kbarticle/Troubleshooting-DC-Agent-with-ConsoleClient

c. Multiple Filtering Service?
   i. Identify the specific Filtering Service filtering the end user.
      1. The block page identifies Filtering Service in URL.
   ii. Identify the Policy Server associated with the Filtering Service.
      1. Each Policy Server should have its own User Service.
      2. Each Policy Server has its own local settings.
      3. See the Filtering Service Summary, on the Today page, to confirm.

d. If the Filtering Service user map is blank – check for communication issues with DC Agent.
   i. TRITON – Web Security manager, select Settings > General > User Identification > Transparent Identification Agents > DC Agent must be listed.
      1. Does the Filtering Service know the DC Agent exists?
         a. Machine names must start with alphabet characters.
         b. Certain extended ASCII characters may not resolve correctly.
         c. Set to an IP address to eliminate DNS issues.
      2. Password.
         a. Must match on DC Agent and FS.
         b. Nothing confidential is passed.
         c. If not using agent authentication, yet the password box is populated, re-enable the feature and clear the box contents.
            i. Leaving content in the password box could prevent DC Agent from passing user names to Filtering Service.

3. Communication ports.
    a. Default ports are 30600 for communications and 30601 for diagnostics.
    b. Filtering Service must be able to contact DC Agent on port 30600.
4. Domain Controller Polling.
    a. Must be enabled.
    b. Default query interval is 10 seconds.
    c. Default entry timeout is 24 hours.
5. Computer Polling.
    a. Enabled by default.
    b. Default verification interval is 15 minutes.
    c. Default entry timeout is 1 hour.
    d. For this feature to be useful, DC Agent must be running with a domain administrator account. All computers must allow DC Agent to access and read their registry.
    e. This feature can be problematic, adding blank names to the user map.
    f. Disable it.
    g. This feature is being re-engineered for v7.6, due out later this year.
    h. Re-evaluate this feature after upgrading to v7.6.
6. Settings marked with an asterisk [“*”] may be altered in a **tranid.ini** file that is specific to each DC Agent.
    a. Check to ensure the **transid.ini** file is not unexpectedly over ridding settings in the TRITON interface.

e. Troubleshooting communications.

i. Any firewalls, IDS's between Filtering Service and DC Agent?
    1. DC Agent server must allow inbound traffic on port 30600.
        a. Telnet from Filtering Service box to DC Agent on port 30600.
            i. **telnet [IP address] 30600**
        b. DC Agent service should be listening on port 30600.
            i. **netstat –ban > ports.txt**
            ii. DC Agent service name is **XidDcAgent.exe**.
            iii. Shows connection to **XidDcAgent.exe** (DC Agent) on port 30600 with Filtering Service (**EIMServer.exe**).
    2. DC Agent server must allow outbound traffic on port: 55815
        a. Telnet from DC Agent box to User Service on port 55815
            i. **telnet [IP address] 55815**
        b. By Default, User Service locates new domain controllers for DC Agent.
ii. Check the **\Websense\bin\Websense.log** file.
    1. Should see a successful connection to 'XID Agent' (DC Agent).
iii. Check the Application Event Log.
iv. Check for Filtering Service, User service, DC Agent hotfixes.
    1. Un-patched v7.5 systems, Filtering Service could lose connection with DC Agent.

If the Filtering Service's user map contains the correct user names, then review the User Service settings in TRION – Web Security.

10. Check for User Service issues—User Service queries your directory service.
    a. Try adding client objects in TRITON – Web Security.
        i. Should be able to display the directory tree.
    b. Review directory service settings in TRITON – Web Security.
        i. Confirm Global Catalog server.
            1. IP address or DNS Alias name entry is preferred.
            2. From a CLI, type:
                a. **telnet <Global Catalog Server> 3268**
        ii. Port usage:
            1. If your directory structure is using a parent/child relationship, ensure port 3268 is used for the parent domain and port 389 for all child domains.
        iii. Is the user account locked out?
        iv. Update the account password.
            1. Most often, the password is not updated.
        v. Check for proper syntax:
            1. domain\administrator
            2. Review the Options tab on the user accounts properties for correct syntax.
        vi. Try using a different domain admin account.
        vii. After any change, try adding client objects in the TRITON interface.
    c. Review Logs.
        i. \Websense\bin\websense.log

ii. Application Event Log.
    1. Look for User Service errors.

d. If you are able to display and add user objects in the TRITON interface, then run a DSTrace to check see what is returned when User Service queries the network for a specific users.
    i. A common problem, at this late point in the troubleshooting process, is that User Service located a duplicate user name.
        1. All user names need to be unique across all domains that Websense is configured to query.
        2. See KB article: "How do I enable DSTrace for UserService?"
            a. http://www.websense.com/support/article/kbarticle/How-do-I-enable-DSTrace-for-UserService
    ii. Nested Groups also may present a problem.
        1. See KB article: "Active Directory Group-Based Policies With Multiple Domains And/Or Nested Groups"
            a. https://emea.salesforce.com/articles/Knowledge_Article/Active-Directory-group-based-policies-with-multiple-domains-and-or-nested-groups?popup=true

When the issue is resolved, TestLogServer should display the correct user name, OU, and LDAP path.

11. Run TestLogServer.
    a. Confirm the expected user name is displayed.
    b. Confirm the OU / LDAP path is correct for the user.
    c. To not lose reporting data while running TestLogServer, see the following article:
        i. How Do I Run TestLogServer Without Stopping Log Server Service?

Additional resources:

- DC Agent troubleshooting (general)
    - http://www.websense.com/support/article/t-kbarticle/v7-DC-Agent-troubleshooting-general-1258048447602
- Troubleshooting DC Agent When Users Are Not Identified
    - http://www.websense.com/support/article/t-kbarticle/v7-DC-Agent-does-not-see-some-or-all-users-1258048446442?popup=true&srPos=0&srKp=kA1
- How Do I Run TestLogServer Without Stopping Log Server Service?
    - To be released soon.
- Troubleshooting DC Agent with ConsoleClient
    - http://www.websense.com/support/article/t-kbarticle/Troubleshooting-DC-Agent-with-ConsoleClient
- Configuring Websense with Your Directory Service
    - http://www.websense.com/support/article/webinar/Webinar-Configuring-Websense-with-your-Directory-Service
- How Do I Enable DSTrace For UserService?

- http://www.websense.com/support/article/kbarticle/How-do-I-enable-DSTrace-for-UserService