User and Group-Based Reporting in TRITON - Web Security: Best Practices and Troubleshooting

Websense Support Webinar March 2012

Support Webinars

web security | data security | email security

Goals and Objectives

websense
ESSENTIAL INFORMATION PROTECTION™

- Directory service configuration
- Delegated administration for reporting
- Reporting on users and groups with presentation and investigative reports
- Common issues with reporting on users and groups
- Troubleshooting
- Best practices for reports on users and groups

Webinar Presenter

Ravi Desai

- Title: Tech Support Specialist
- Accomplishments:
  - Over 4 years supporting Websense products
- Education / Certifications:
  - B.Eng (Hons) Computer Systems and Networks
  - MCP
  - CCNA
  - WCWSA (Websense Certified Web Security Associate)
- Qualifications:
  - New Hire Training
  - v7 Tech Support Training

Directory Service Configuration

websense
ESSENTIAL INFORMATION PROTECTION™

- User Service communicates with a supported LDAP or NTLM directory service.
  - Passes information from the directory service to Policy Server and Filtering Service to apply policies to users, groups, and organizational units (OUs)
  - Communicates with Log Server to provide updated user and group information
- Configure User Service settings for end users and administrators.
  - Configure the directory for end users on the Settings > Directory Services page in TRITON - Web Security.
  - Configure the administrator directory on the TRITON Settings > User Directory page.
- Duplicate user names are not supported for LDAP directories. The same user must not appear in multiple domains.

Directory Service Configuration

- Use the Active Directory (Native Mode) option to configure multiple domains.
  - Use DNS names when the environment includes multiple domains.
- For Active Directory (Mixed Mode), make sure the group scope is set to Global. (Universal groups do not work with mixed mode.)
- When configuring any other LDAP-based directory, use port 389 with an appropriate root context.
- If the directory structure contains duplicate users, configure the **UseDomainMap** parameter in **websense.ini**.

Delegated Administration for Reporting

- Delegated administrators can be granted specific reporting permissions.
  - Configure administator permissions on the Policy Management > Delegated Administration > Add Role or Edit Role page in TRITON - Web Security.
- 2 types of roles can be created: **policy management and reporting** or **investigative reporting only**.
- The account type can be network or local.
- You can control whether administrators assigned to a role can report on no clients (no reporting permissions), only clients in the role, or all clients.

User and Group Reports

- Presentation reports
  - Use pre-defined templates for reporting
  - Can generate charts and tabular reports in HTML, PDF, or XLS format
  - Reports include:
    - User Activity Detail and User Activity Summary
    - Top Users and Groups by Request
    - Top Users and Groups by Browse Time
    - Top Users and Groups by Bandwidth
  - Can be scheduled to run daily, weekly or monthly
  - Cannot run debug against these reports

User and Group Reports

- Investigative reports
  - Interactive reporting used to analyze filtering activity
  - Can generate summary report based on particular user or group name
  - Report can be saved as a Favorite to run or schedule later
  - Can enable debug for individual reports to find out which query is used to process data

Common Issues

- Blank user and group based reports: no data
- No user names in reports
- Delegated administrators cannot report on managed clients
- Delegated administrator reports run slowly
- Group-based reports do not show all AD groups
- Group-based reports do not contain all users
- Reports show incorrect group membership

Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Tables related to user and group reporting in Microsoft SQL Server
  - **Users**: Contains user-related data passed by User Service to Log Server. Contains the unique user_id associated with each user record.
  - **user_groups**: Used to track group membership. Contains user and group update data. The start_dates and end_dates are used to pull user data into group reports based on date range.
  - **wse_domains**: Contains information about domain objects such as OUs with their relevant domain ID.
  - **wse_group_domains**: Contains information on groups associated with a particular AD domain. Displays the date the group information was created in the Log Database.

Troubleshooting

- Database contains views with user and groups information

  user_names: Built using information from the users table. Contains more detailed logs of user-related data

  groups: Contains information on various groups obtained by Log Server. Each group has a unique ID.

Results | Messages

	user_id	user_name	user_login_name	user_full_name	namespace	user_display_name	catalog_server	last_update	domain
1	1	10.5.146.47	10.5.146.47	10.5.146.47		10.5.146.47	NULL	2011-12-06 12:18:20.797	
2	2	CN=Users,DC=uklab-ws,DC=com /	Administrator		LDAP	[Administrator]	10.5.144.100	2012-03-08 01:24:00.000	CN=Use
3	3	10.5.146.50	10.5.146.50	10.5.146.50		10.5.146.50	NULL	2011-12-12 16:17:20.793	
4	4	OU=Mark Hybrid 2,DC=uklab-ws,DC=com / Hybrid2, M...	mhybrid2	Hybrid2, Mark	LDAP	Hybrid2, Mark[mhybrid2]	10.5.144.100	2012-03-08 01:24:00.000	OU=Mar

	group_id	group_name	group_domain	domain_id
1	1	Administrators	CN=Builtin,DC=uklab-ws,DC=com	2
2	8	Performance Monitor Users	CN=Builtin,DC=uklab-ws,DC=com	2
3	14	Users	CN=Builtin,DC=uklab-ws,DC=com	2

Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Blank user and group reports
  - Run the TestLogServer utility to see if user names are associated with each filtering request.

  Kb Link: http://www.websense.com/support/article/t-kbarticle/Using-TestLogServer-with-Websense-Enterprise
  - Run a User Service trace (dstrace) to see if user and groups are being picked up correctly.
  - Verify that Log Server is configured to log user names.
  - Check the user and groups tables in SQL Server. Verify the last_update column to ensure that users have been updated.

Troubleshooting

- No user names in reports
  - Verify that user-based filtering policies are being applied correctly.
  - Run the TestLogServer utility to see if user names are associated with each filtering request.
    - If no user names are seen in TestLogServer, there is likely a user identification issue. Check your user identification settings.
    - If user names do appear , check connectivity between User Service and Log Server.
  - Run Log Server debug.

Troubleshooting

Running Log Server debug

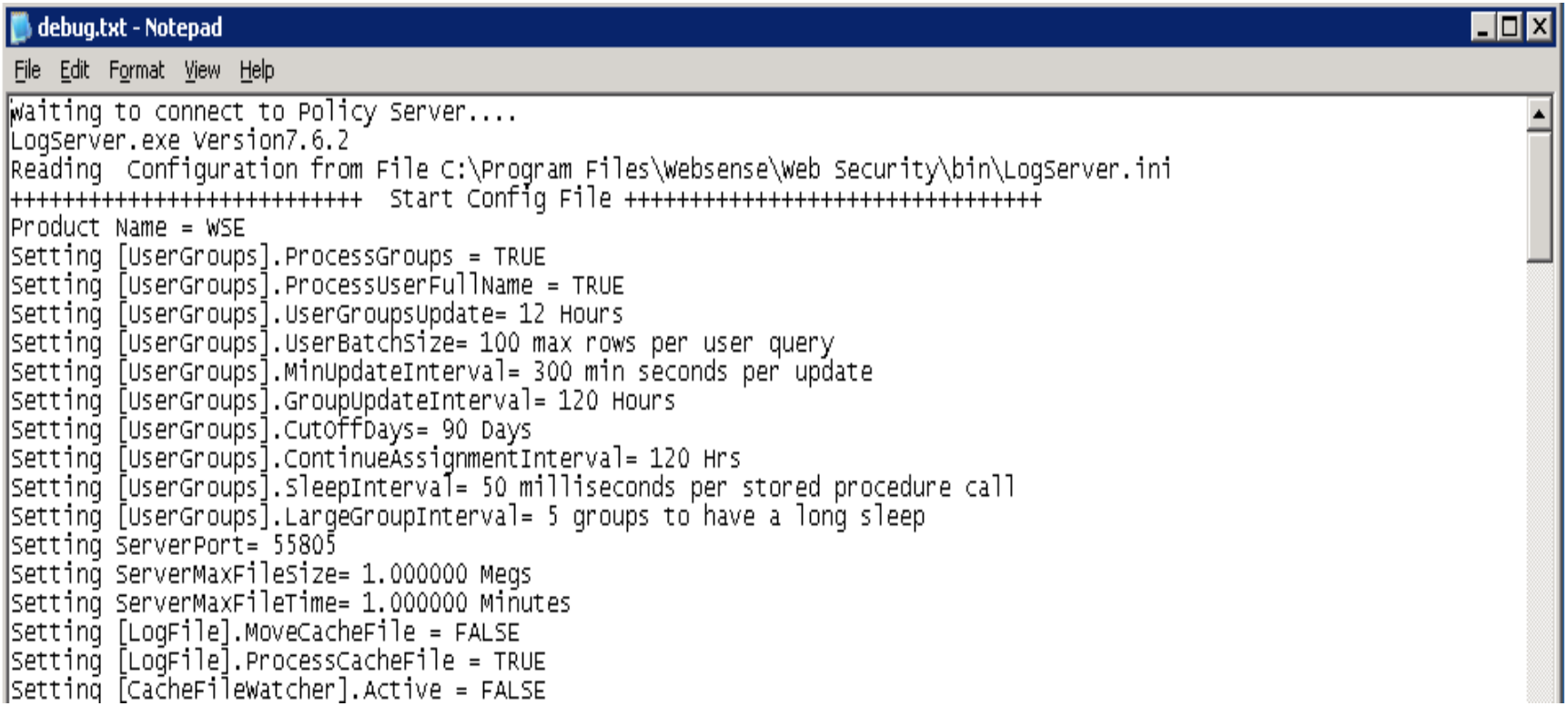
1. Use the Services utility (Start > Administrative Tools > Services) to stop the **Websense Log Server** service.
2. Right-click the service name and click **Properties**.
3. On the General tab, next to **Start parameters**, enter:

   `-debug`
4. Use the Properties dialog box to start Log Server.
5. A **debug.txt** file is created in the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin, by default).
6. Analyze the file for errors related to User Service update failures.

Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Log Server debug file
  - The start of the debug file shows some important parameters related to user and group update intervals.



Troubleshooting

- Log Server debug file
  - Look for user and group update failure messages

debug.txt - Notepad

File Edit Format View Help

```
NY,OU=USA,DC=NOAM,DC=xyz,DC=com/02HW8499 DB.USER_ID = 7776--
wsUserServiceHelper::GetFullUserName - FAILURE LDAP://172.50.96.24 OU=Laptops,OU=Computers,OU=Edison - NJ,OU=NEW YORK 1 - NY,OU=
USA,DC=NOAM,DC=xyz,DC=com/02HW8499 status[826802196]
wsUserServiceHelper::GetFullUserName - FAILURE LDAP://uscinsevdc1 OU=Laptops,OU=Computers,OU=Edison - NJ,OU=NEW YORK 1 - NY,OU=
USA,DC=NOAM,DC=xyz,DC=com/02HW8499: Blank user full name.
wsUpdateGroupThread::execute - ERROR: Failed to query US for username: LDAP://uscinsevdc1 OU=Laptops,OU=Computers,OU=Edison - NJ,OU= NEW
YORK 1 - NY,OU=USA,DC=NOAM,DC=xyz,DC=com/02HW8499. Skip this user.
wsConvertThread::doProcessFile EOF marker for C:\Program Files\Websense\bin\Cache\logCB29.tmp : 10.102.48.241 : 1331121754
3/7/2012 7:05:56 AM wsConvertThread::doProcessFile - Finished Processing File C:\Program Files\Websense\bin\Cache\logCB29.tmp - 0 Seconds
wsUpdateGroupThread::execute: - Process DomainUser: LDAP://172.50.96.24 OU=Servers,OU=Computers,OU=Edison - NJ,OU=NEW YORK 1 - NY,OU=
USA,DC=NOAM,DC=xyz,DC=com/USTROYDHCP DB.USER_ID = 7771--
3/7/2012 7:05:56 AMwsVisitHitThread::doProcessNextRec received EOF marker for C:\Program Files\Websense\bin\Cache\logCB29.tmp
wsUserServiceHelper::GetFullUserName - FAILURE LDAP://172.50.96.24 OU=Servers,OU=Computers,OU=Edison - NJ,OU=NEW YORK 1 -
NY,OU=USA,DC=NOAM,DC=xyz,DC=com/USTROYDHCP status[826802196]
wsUserServiceHelper::GetFullUserName - FAILURE LDAP://uscinsevdc1 OU=Servers,OU=Computers,OU=Edison - NJ,OU=TCS - NEW YORK 1 - NY,OU=
USA,DC=NOAM,DC=xyz,DC=com/USTROYDHCP: Blank user full name.
wsUpdateGroupThread::execute - ERROR: Failed to query US for username: LDAP://uscinsevdc1 OU=Servers,OU=Computers,OU=Edison - NJ,OU=| NEW
YORK 1 - NY,OU=USA,DC=NOAM,DC=xyz,DC=com/USTROYDHCP. Skip this user.
```

Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Running dstrace to debug User Service

1. Add the following lines to the **websense.ini** file:

```
[DirectoryService]
GroupLog=true
BindLog=true
CacheLog=true
```

2. Restart Websense User Service.

   A **dstrace.txt** file is created in the **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/, by default).

2. Check the file to see if user and group information has been correctly obtained by User Service.

Troubleshooting

- Using SQL queries to verify data in the Log Database.
  - To find a record for a specific user (like “Administrator”) within the database:

    ```
    select * from users where user_login_name like 'Administrator'
    ```

  - Check the last_update column to ensure that user information is being updated.
  - To find information related to a specific group (like “Domain Admins”):

    ```
    select * from groups where group_name like 'domain admins'
    ```

Troubleshooting

- Use the user_id and group_id fields to see if user and group data has been updated
  - For example, verify that user Administrator is associated with group Domain Admins and group data is updated.

    ```
    select * from user_groups where group_id = '3' AND user_id = '2'
    ```
  - end_date is the last date the user is considered a member of the group. It is updated when Log Server gets an update from User Service. The date is in the future if membership is ongoing.

Results | Messages

	start_date	end_date	user_id	group_id
1	2011-12-12 16:16:00.000	2012-03-13 01:24:00.000	2	3

Troubleshooting

- If delegated administrators cannot report on their managed clients:
  - Check administrator permissions for the role.
  - When an administrator runs a report on managed clients, a view is created in SQL Server for that administrator role. If the assigned administrator does not have permission to report on those clients, the view will not be created.
  - The Investigative Reports page can be used to debug the report that is being generated:
    - Switch to full screen view and add **&gubed=1** to the end of the UR in the address bar.
  - Check dbo.directory_object table in the Log Database and verify that the correct context exists.

Troubleshooting

- If group reports don't show all AD groups or all users for a specific group:
  - Run **dstrace** to verify that User Service can obtain information from AD for all groups.
  - Run Log Server debug to verify that User Service can update Log Server.
  - Check the last_update field in the users table to verify that user information has been updated in the Log Database.
  - Check the start_date and end_date columns in the user_groups table to verify relevant group information has been updated.

Troubleshooting

- If group reports show incorrect group membership for users:
  - Run **dstrace** and verify that User Service can obtain correct group membership with a NetGetGroup query.
  - If the user has been moved from one group to another, ensure that User Service gets the new membership.
  - Verify that the user_id is associated with relevant group_id in the user_groups table in the database.

Troubleshooting

- Check the start_date and end_date data, and compare it to the date range of the report.

- If Log Server didn't gather user data on the day the group membership changed, the end_date will be past the true end date. Log Server uses the current date and time as the end_date when it discovers that group membership has ended.

- If user A belongs to Group1 from 1/1 to 2/20 and the report dates are 2/1 to 28, user A is considered part of Group1 for all of the report data.

Best Practices for User group Reporting

- Configure directory service settings correctly based on the directory structure.
- Ensure that User Service can communicate with the relevant global catalog servers to obtain necessary user and group information.
- User Service and Log Server services must be able to communicate.
- If users move frequently from one group to the other within the directory, consider lowering the User Service cache timeout period.
- Take older partitions offline to speed report generation, especially for delegated administrators.

Best Practices for User group Reporting

websense
ESSENTIAL INFORMATION PROTECTION™

- For larger organizations, consider rolling over partitions by size to ensure each partition db does not grow to an enormous size
- If databases have grown very large consider adding more physical drives to the SQL server machine to store the log files, this will enhance performance
- Run perfmon on SQL server to view disk performance if reporting seems to be generally slow
- Ensure tempdb has enough space allocated to it as this will be needed especially with delegated admin reporting

Support Online Resources

websense
ESSENTIAL INFORMATION PROTECTION™

Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

Tech Alerts

- Subscribe to receive product-specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

ask.websense.com

- Create and manage support service requests using our online portal.

Webinar Announcement

websense
ESSENTIAL INFORMATION PROTECTION™

Webinar Update

Title: **Filtering remote users with Websense remote filtering software v7.6**

Date: April 18, 2012

Time: 8:30 AM Pacific Time

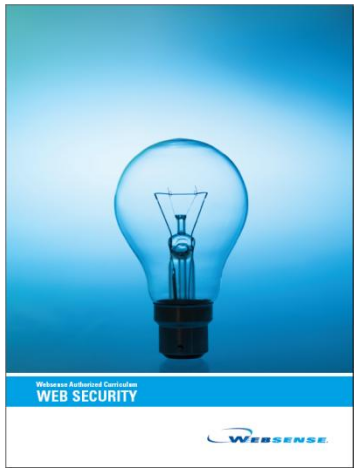
How to register:
http://www.websense.com/content/SupportWebinars.aspx

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass
- Websense Training Partners also offer classes online and onsite at your location
- For more information, please send email to: readiness@websense.com

WEBSENSE® Authorized Training Partner

WEBSENSE® Certified Instructor



Questions?