Highlights of WebSAMS Server, Network & Security Seminar
Contents:

- WebSAMS Architecture
- Security and Maintenance
- Backup of Data
- Logs Checking
- Root Certificate & SSL Certificate
- Regular Checking of WebSAMS System Security Settings
WebSAMS Architecture
WebSAMS Requirements

- WebSAMS Network is a private and separated network, isolated from ITED Network
- Outside the WebSAMS Network, all users must go via the HTTP Server to access WebSAMS
- HTTP Server can be located within the Demilitarized Zone (DMZ) zone, or inside the ITED Network, as shown in the following page
WebSAMS Requirements

- HTTP Server and WebSAMS Server are connected in different subsets.

- Required software is installed in WebSAMS server
  - Apache
  - Jboss & JRE (Java)
  - Sybase SQL Anywhere 16
  - Crystal Server 2013
  - Anti-Virus Software & Backup Software

- All WebSAMS network card must be connected to WebSAMS network only.
Design A: Internet Gateway without DMZ
Network Designs in WebSAMS (cont’d)

Design B: Internet Gateway with DMZ

[Diagram showing network architecture with DMZ, HTTP Server, Web/Email/Proxy Server, Internet Gateway/Firewall, WebSAMS switch, WebSAMS router, ITED switch, and related components.]
Internet Gateway

- Separate Internet and ITED
  - 2 interfaces - one for real IP and another for internal IP
- Support NAT (Network Address Translation), i.e. access from Internet to ITED
What is NAT?

- Network Address Translation (NAT)
- Translate the IP address from one network to other network
  - Typically one is inside and one is outside
- Port mapping function
HTTP Server

- HTTP server is simply a relay server which forwards all the requests to the WebSAMS server.

- The HTTP server itself does not store any data.

WebSAMS Architecture

**Design B: Internet Gateway with DMZ**

Diagram showing the setup of the Internet Gateway with DMZ, including the Internet User, ISP equipment, School Premise, DMZ, HTTP Server, Web / Email / Proxy Server, WebSAMS Server, WebSAMS switch, WebSAMS router, ITED switch, and ITED PCs.
**Design B: Internet Gateway with DMZ**

![Diagram showing a network setup with WebSAMS Router and WebSAMS Architecture](image)
WebSAMS Router (cont’d)

- WebSAMS Router (between WebSAMS and ITED)
  - *Block all unnecessary network traffic
  - *Only allow specific network services and TCP ports
  - HTTP Server connects to WebSAMS server
  - WebSAMS server can access Internet without passing through proxy
  - For details of configurations of WebSAMS Router and School Internet Gateway, please refer to ‘Doc 36 - Rules for Configuration of WebSAMS Router and Internet Gateway’
Security and Maintenance
Best practices on protection of and export of data from WebSAMS:

- Proper Access Control
- Data Encryption
- Password Handling

- Disable remote desktop service in WebSAMS server
Patch update

- Update security patches of Windows Server 2012R2
- Install major Windows patches for Window Servers only after testing by EDB as announced via WebSAMS Release Notes / CDR message from time to time
- Enable real time protection & update virus pattern on Anti-virus program (including all server and workstation)
- Update IOS (Cisco) or firmware on WebSAMS Router (Consult to hardware vendor)
- Command “starthsp” can be completed successfully in HTTP server
Data Security

- Disconnect any shared folder on WebSAMS Server
Data Security (cont'd)

- NAS should be connected to WebSAMS Server with a cross-over ethernet cable. Do not connect NAS device to the WebSAMS network switch.
- Exposure of any sensitive export data to any public machine, such as student & guardian personal info, staff personal info, financial report, etc. is not recommended.
- Keep an offline and offsite backup
Data Security (cont'd)

- Keep original basic network setting in WebSAMS unchanged. For example:
  - Do not connect WebSAMS Server to the ITED network switch or firewall directly.
  - Do not connect WebSAMS HTTP Server to the WebSAMS network switch.
  - Do not connect NAS device to WebSAMS network switch.
  - Do not connect Internet cable from ISP to WebSAMS Server.
To protect against leakage of sensitive data, schools are advised to:

- ensure that users can only import and export system data when they are authorized to do so and appropriate measures have been taken.

- maintain accuracy, integrity and consistency of system data when importing data to WebSAMS

- take all feasible measures so as to ensure the personal data collected by data users are protected against unauthorized or accidental access, processing, erasure or use.
Resources on IT Security of WebSAMS

**IT Security in Schools – Recommended Practice (ITSS):**
- Path: EDB Webpage > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education > On-going Support

**Security Guides & Checklist for WebSAMS:**
- Path: http://cdr.websams.edb.gov.hk > 主頁 > 參考資料 > 保安及處理敏感數據指引

**WebSAMS Version Upgrade release note:**
Security & Maintenance

- Security reminders in security alert from EDB from time to time
  - Path: *EDB Website > Education System and Policy > Primary and Secondary School Education > Applicable to Primary and Secondary School > IT in Education*

- Regularly visit the Information Security website of HKSAR for the update information of IT security
  - [http://www.infosec.gov.hk](http://www.infosec.gov.hk)

- Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
  - [https://www.hkcert.org](https://www.hkcert.org)
Only open WebSAMS to Internet access for a specific period when necessary:

1. Restrict the time for accessing WebSAMS from clients outside SAMS LAN segment at “Security > Configuration > System Configuration”
2. Set up specific “Internet Access Time Profile” to further control the access time for particular user clients outside SAMS LAN segment at “Security > Access Control > Internet Access Time Profile”
### Internet Access Time Profile

**Profile Description**
- **Student TEST**
- **Student Access Time Period**

**Chinese Profile Description**
- 學生使用時段

<table>
<thead>
<tr>
<th>Weekday</th>
<th>Period</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>From (DD/MM/YYYY)</td>
<td>01/09/2011 To 31/08/2012</td>
</tr>
<tr>
<td></td>
<td>To (DD/MM/YYYY)</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Monday - Friday</td>
<td>From (DD/MM/YYYY)</td>
<td>08:30 To 17:00</td>
</tr>
<tr>
<td>Saturday</td>
<td>From (DD/MM/YYYY)</td>
<td>08:30 To 13:00</td>
</tr>
</tbody>
</table>

**Note:**
2. Internet Access Time Profile can contain only the characters of a-z, A-Z, 0-9, "," or ":".
OS Hardening Setting and Security Best Practices:

1. Local Security Policy
   - Start Control Panel -> Administrative Tools -> Local Security Policy
   - In Account Policies -> Account Lockout Policy, set Account lockout threshold to "3" invalid logon attempts
   - Set Account logout Duration and also Reset account lockout counter after to "30 minutes".
WebSAMS Server Security (cont'd)

Security & Maintenance

- In Local Policies -> Audit Policy

- Set Audit object access security setting to "Failure" and also set Audit system events security setting to "Success"

- More policy settings in Appendix 8 of Installation Guidelines for WebSAMS 3.0
2. User account management

- **Disable / delete all unused Login Accounts of Windows Server and WebSAMS Application**

- **Start -> Control Panel -> Administrative Tools -> Computer Management -> System Tools -> Local Users and Groups -> Users -> Administrator**

- **On the General tab of ALL user accounts properties, uncheck the Password never expires checkbox.**
3. Enable Screen Saver Timeout

- **WebSAMS Server**

- Similar settings also apply to WebSAMS workstation/ITED workstation if accessing WebSAMS

  - *Start* -> *Control Panel* -> *Display* > *Change screen saver*
4. Enable Windows Firewall

- **Start -> Control Panel -> Windows Firewall -> Advanced**
Inbound Rules > new Rule...

1. Inbound Rules
2. New Rule
Rule Type > Port

1. Rule Type

2. Port
   Rule that controls connections for a TCP or UDP port.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

- Program
  Rule that controls connections for a program

- Port
  Rule that controls connections for a TCP or UDP port.

- Prgdefined:
  Active Directory Web Services

- Custom
  Custom rule.

< Back  Next  >  Cancel
Protocol and Ports > TCP > Specific local ports:

- 80, 443, 8009, 7009, 3268, 7010, 7268 (Add 8109 & 9268 for 1 Server 2 WebSAMS only)
WebSAMS Server Security (cont'd)

- Action > Allow the connection

1. 

2. 

New Inbound Rule Wizard

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

**Steps:**

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

- **Allow the connection**
  This includes connections that are protected with IPsec as well as those that are not.

- **Allow the connection if it is secure**
  This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

- **Block the connection**
Profile > Domain, Private & Public

1. Profile
2. New Inbound Rule Wizard

- **Domain**: Applies when a computer is connected to its corporate domain.
- **Private**: Applies when a computer is connected to a private network location, such as a home or work place.
- **Public**: Applies when a computer is connected to a public network location.
**WebSAMS Server Security** (cont'd)

- Name > WebSAMS > Finish

1. **Name**
2. **WebSAMS**
3. **Name**
4. **WebSAMS**
5. Apply Latest Security patch of WebSAMS
Backup of Data
Backup

** Remind: Importance of Regular Off-Line Backup

WebSAMS Backup Schedule
- Pre-backup → Backup → Post-backup
- From about 00:00 am to 06:00 am

Flow of Scheduled Backup:
- Stop WebSAMS engine
- Backup
- Housekeep WebSAMS application log files
- Start WebSAMS engine

Encryption of backup images
Backup Job Workflow

1. Shutdown Apache
2. Shutdown Jboss/Tomcat
3. Shutdown Database
4. Backup C: Drive (Operating System)
5. Backup D: Drive (Application)
6. Backup E: Drive (Database)
7. House keep Apache Log
8. House keep Server Log
9. House keep CDS Log
10. House keep Report Temp Files
11. Start Apache
12. Start DB
13. Start JBoss / Tomcat
Pre-backup

- D:\WebSAMS3.0\batch\pre_backup.bat

- 15 mins

- Stop JBoss, database, Apache

- Make copy of WebSAMS data to
  - E:\data\<SUID>\database\sched
Post-backup

- **Backup of Data**
  - D:\WebSAMS3.0\batch\post_backup.bat

- **Housekeep Apache log files**
  - D:\WebSAMS3.0\Apache\logs

- **Housekeep WebSAMS server log files (older than 30 days)**
  - D:\WebSAMS3.0\JBoss-as-7.1.1.Final\standalone\log

- **Housekeep CDS log (More than 30 days)**
  - E:\data\CDS\<dest_id>\system\log

- **Housekeep Report temp log files**
  - E:\data\<SUID>\rpt\temp

- **Start database, JBoss, Apache**
Backup on HTTP Server

- Back up WebSAMS HTTP server (SUSE Linux Enterprise 11) setting to a USB drive or a floppy drive
  
  - User command “httpconfig”
  
  - Or use command “fdisk -l” to check USB device name e.g.: sda1, sda2 or sdb1...,etc.
  
  - Use command “grepconfig” / “grepconfig /dev/{USB device name}”.
    (For 1 Server 2 WebSAMS environment, use “grepconfig_1s2s”)
  
- Run the command when HTTP server is running in good condition

- Those files can be copied to any Windows storage for backup purpose
Backup on HTTP Server (cont'd)

- Step 1: Log in HTTP server as root

- Step 2: Type command "httpconfig"

- Or "grepconfig /dev/sda1".

- Step 3: Press "Y" in the following screen

```
Please insert USB Flash Drive / Floppy Diskette and then select option:

1) USB Flash Drive
2) Floppy Diskette
q) Quit

>1
Please wait 5 seconds for detecting the USB flash drive ....
```
Backup on HTTP Server
(cont'd)

This program will help you to grep collect all the information from your current HTTP server to a floppy so that you can use it after reinstallation of Linux.

Before you continue, please confirm if your HTTP server meet ALL the following prerequisite:

1. Your HTTP server is a functional WebSAMS HTTP server;

2. Your HTTP server is NOT act as a NAT server for WebSAMS server to access Internet;

3. Your HTTP server has ONLY 1 IP address.

Confirm? (y/n) _
Backup on HTTP Server (cont'd)

- Step 4: Press “0” if all information is correct
- Step 5: Press “Y” to confirm in the following screen

Current HTTP Server Configuration

1. Hostname: HTTP
2. IP: 192.168.2.211
3. netmask: 255.255.255.0
4. gateway: 192.168.2.1
5. DNS: 192.168.1.204
6. WebSAMS IP: 192.168.3.111
7. Router ITED Leg: 192.168.2.254
8. FQDN: websams.abcschool.edu.hk
9. SUID: 1234

Choose 1 - 9 for Modification, or enter 0 if All Information is Correct: 0
Confirm to copy configuration and files into the floppy? (y/n) _
Logs Checking
Logs checking

- Windows Event Viewer log
  - Control Panel > Administrative Tools > Event Viewer

- Apache log
  - D:|WebSAMS3.0|Apache|logs|
    - access.log- <dd-MM-yyyy> (http request log)
    - errors.log- <dd-MM-yyyy> (error log)

- Virus scanning log

- Backup software log
Logs checking (cont'd)

- Local backup log
  - To check whether the pre-backup tasks have been run successfully (E:\data\<SUID>\Log\DB\backup.log)

<table>
<thead>
<tr>
<th>Backup Time</th>
<th>WebSAMS Version</th>
<th>DB Service</th>
<th>DB Schema Version</th>
<th>Backup Location</th>
<th>Backup Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Sep 16 18:53:48</td>
<td>3.0.0.28082015</td>
<td>websams_8886</td>
<td>3.0.0.011</td>
<td>E:\data\8886\database\sched\</td>
<td>successful</td>
</tr>
<tr>
<td>Wed Sep 16 18:33:23</td>
<td>3.0.0.28082015</td>
<td>websams_8886</td>
<td>3.0.0.011</td>
<td>E:\data\8886\database\adhoc\</td>
<td>successful</td>
</tr>
<tr>
<td>Tue Sep 15 01:44:40</td>
<td>3.0.0.28082015</td>
<td>websams_8886</td>
<td>3.0.0.011</td>
<td>E:\data\8886\database\sched\</td>
<td>successful</td>
</tr>
<tr>
<td>Mon Sep 14 01:14:08</td>
<td>3.0.0.28082015</td>
<td>websams_8886</td>
<td>3.0.0.011</td>
<td>E:\data\8886\database\sched\</td>
<td>successful</td>
</tr>
<tr>
<td>Sun Sep 13 01:13:31</td>
<td>3.0.0.28082015</td>
<td>websams_8886</td>
<td>3.0.0.011</td>
<td>E:\data\8886\database\sched\</td>
<td>successful</td>
</tr>
</tbody>
</table>
Logs checking (cont'd)

- JBoss Server Log
  - D:\WebSAMS3.0\JBoss-as-7.1.1.Final\standalone\log\server.log

![Server Log Example]

- **Severity**
- **Time Stamp**
- **Message**
Logs checking (cont'd)

- WebSAMS Upgrade Logs
  - E:\temp\sup1\<yyyyMMdd.HHmm>\*
  - E:\temp\sup2\<yyyyMMdd.HHmm>\*
    (For 2nd instance of 1 Server 2 WebSAMS)
  - E:\temp\training\<yyyyMMdd.HHmm>\*
  - Files and directories are saved under <yyyyMMdd.HHmm> folder, and the latest folder should be kept for tracking purpose.
Logs checking (cont'd)

- **WebSAMS HTTP Linux Server**
  - Apache log
    - (/var/log/apache2/access_log_80, 443, 7010)
  - Error log
    - (/var/log/apache2/error_log_80, 443, 7010)
  - System log
    - (/var/log/messages)
  - Virus scan log
    - (/var/log/TrendMicro/SProtectLinux/Virus.yyyyMMdd.#####)
Logs checking (cont'd)

- **Linux System Log**
  - `/var/log/messages`
  - `/var/log/`
Logs checking (cont'd)

- All logs in anti-virus:
  - https://websams.school.edu.hk:14943
  - Virus Logs, Spyware Logs, Scan Logs & System Logs
  - /var/log/TrendMicro/SProtectLinux/

![Trend Micro ServerProtect](Trend%20Micro%20ServerProtect.png)
### System Logs

**Data Range:** 2009-08-31 15:45:02 to 2009-09-02 16:18:00

#### Logs Checking

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Description</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-09-02</td>
<td>Real-time scan has been enabled.</td>
<td></td>
</tr>
<tr>
<td>16:18:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-02</td>
<td>Real-time scan has been disabled.</td>
<td></td>
</tr>
<tr>
<td>16:16:02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-02</td>
<td>Real-time scan has been enabled.</td>
<td></td>
</tr>
<tr>
<td>00:00:16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-02</td>
<td>ActiveUpdate Success</td>
<td>Virus Pattern 6.407.00 to 6.411.00; Spyware Pattern 0.817.00 to 0.817.00, Engine 8.7.1004 to 8.7.1004</td>
</tr>
<tr>
<td>00:00:16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-02</td>
<td>Real-time scan has been disabled.</td>
<td></td>
</tr>
<tr>
<td>00:00:07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-01</td>
<td>License update successful</td>
<td>The license expiration date has been extended until 2010-08-31</td>
</tr>
<tr>
<td>01:30:02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-01</td>
<td>Real-time scan has been enabled.</td>
<td></td>
</tr>
<tr>
<td>01:02:26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-01</td>
<td>ActiveUpdate Success</td>
<td>Virus Pattern 6.397.00 to 6.407.00; Spyware Pattern 0.813.00 to 0.817.00, Engine 8.7.1004 to 8.7.1004</td>
</tr>
<tr>
<td>01:02:26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-09-01</td>
<td>Real-time scan has been disabled.</td>
<td></td>
</tr>
<tr>
<td>01:02:18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009-08-31</td>
<td>Real-time scan has been enabled.</td>
<td></td>
</tr>
<tr>
<td>15:45:02</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logs checking (cont'd)

- **Hardware Firewall Log Screen**

  ![Hardware Firewall Log Screen](image-url)
Change password

- Change Passwords in regular basis
  - OS System administrator
  - WebSAMS login accounts including “sysadmin” and “asysadmin”
  - HTTP root account

![Local Security Policy]

- Enforce password history: 5 passwords remembered
- Maximum password age: 100 days
- Minimum password age: 3 days
- Minimum password length: 8 characters
- Password must meet complexity requirements: Enabled
- Store passwords using reversible encryption: Disabled
### Change password (cont'd)

#### Logs Checking

![Change password interface]

<table>
<thead>
<tr>
<th>General Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum number of fault login attempts allowed</strong></td>
</tr>
<tr>
<td>(Zero for no limitation, default value: 3)</td>
</tr>
<tr>
<td><strong>Auto-unlock period of locked accounts</strong></td>
</tr>
<tr>
<td>(Zero for no auto-unlock, default value: 15 hours)</td>
</tr>
<tr>
<td><strong>Automatic logout period (inside SAMS LAN Segment)</strong></td>
</tr>
<tr>
<td>(Maximum: 180 minutes, default value: 15 minutes)</td>
</tr>
<tr>
<td><strong>Automatic logout period (outside SAMS LAN Segment)</strong></td>
</tr>
<tr>
<td>(Maximum: 120 minutes, default value: 5 minutes)</td>
</tr>
<tr>
<td><strong>Password expiry period</strong></td>
</tr>
<tr>
<td>(Zero for no expiry, default value: 100 days)</td>
</tr>
<tr>
<td><strong>Number of passwords stored in password History</strong></td>
</tr>
<tr>
<td>(Min: 1, Max: 5, default value: 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Multiple Login</strong></td>
</tr>
<tr>
<td>(Default: disabled)</td>
</tr>
<tr>
<td><strong>Enable Internet Access</strong></td>
</tr>
<tr>
<td>(Default: disabled)</td>
</tr>
<tr>
<td><strong>Enable ITED Access</strong></td>
</tr>
<tr>
<td>(Default: disabled)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path of Data Backup Log File</strong></td>
</tr>
<tr>
<td>E:\DATA\8886\LOG\DB\</td>
</tr>
<tr>
<td><strong>Path of Server Backup Log File</strong></td>
</tr>
<tr>
<td>E:\DATA\8886\LOG\SR\</td>
</tr>
<tr>
<td><strong>Path of Archive File</strong></td>
</tr>
<tr>
<td>E:\DATA\8886\SEC\AUDIT\</td>
</tr>
</tbody>
</table>
Root Certificate & SSL Certificate
Purpose of installing root certificate:

With this root certificate, WebSAMS is confirmed as a trusted website. No more warning message will be shown whenever accessing WebSAMS again.
Install WebSAMS Root Certificate on Windows Vista/7/8/10

- Root certificate on WebSAMS client PC

Root Certificate & SSL Certificate
Install WebSAMS Root Certificate on Windows Vista/7/8/10
Root certificate on WebSAMS client PC (cont'd)

- Install WebSAMS Root Certificate on Windows Vista/7/8/10
Root certificate on WebSAMS client PC (cont'd)

- Install WebSAMS Root Certificate on Windows Vista/7/8/10
Root certificate on WebSAMS client PC (cont'd)

- Install WebSAMS Root Certificate on Windows Vista/7/8/10
Root certificate on WebSAMS client PC (cont'd)

- Verification of root certificate in Internet Explorer
  - Tools (Alt+T) > Internet Options > Content tab
Root certificate on WebSAMS client PC (cont'd)

- Verification of root certificate in Internet Explorer
Upgrade of SSL Certificate in WebSAMS HTTP Server

- Browser providers may terminate the old Security Sockets Layer (SSL) Certificate at any time

- Ensure school’s WebSAMS network would not be susceptible to security risks

- For details, please refer to the CDS message on 29 November, 2016 “Important Upgrade of SSL Certificate in WebSAMS HTTP Server”
Regular Checking of WebSAMS System Security Settings
System Security Setting Checklist for WebSAMS (cont'd)

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Item Description</th>
<th>Checking Items</th>
<th>Checking Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WebSAMS Server and Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>IP Address of ALL Network Cards in WebSAMS Server (IP addresses must be under WebSAMS subnet ONLY)</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>IP Address of Default Gateway of WebSAMS Server (It must be the IP Address of WebSAMS Router)</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Regular change of all Login Passwords of Windows Server and WebSAMS Application</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Disable / delete all unused Login Accounts of Windows Server and WebSAMS Application</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Only the following software is installed in WebSAMS server:</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Apache</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• JRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sybase SQL Anywhere 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Crystal Server 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Anti-Virus Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Backup Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Virus Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Real-time Protection is enabled</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Auto-update of virus definition is enabled, and Last Update Date of virus definition</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup Software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Regular Backup Job is scheduled</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Encryption of backup image is enabled, and Last Successful Backup Date</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review OS Hardening Setting (Please refer to Appendix 7 of &quot;Installation Guidelines for WebSAMS, 3rd&quot;)</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Local Security Policy is set</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote Desktop should be disabled</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Screen Saver Timeout is enabled</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• with displaying Logon Screen on resume</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Firewall is enabled</td>
<td>☐ Yes ☐ No</td>
<td></td>
</tr>
</tbody>
</table>

| 2        | HTTP Server | | |
| 2.1      | IP Address of HTTP Server | (Please type command "grepconfig" and then refer to item 2 in the displayed configuration list) | ☐ Yes ☐ No |
| 2.2      | Environment of the HTTP Server | | |
|          | • HTTP Server and WebSAMS Server are connected in different subnets | ☐ Yes ☐ No |
|          | • The command "startups" can complete successfully. (Please refer to Section 8.7.2 of "Installation Guidelines for WebSAMS, 3rd") | ☐ Yes ☐ No |
| 2.3      | Anti-Virus Software of the HTTP Server | | |
|          | • "Real-time Scan" is enabled (Please refer to Section 8.7.2 - 1c of "Installation Guidelines for WebSAMS, 3rd") | ☐ Yes ☐ No |
|          | • The software license is active (Please refer to Section 8.7.1 - 2d of "Installation Guidelines for WebSAMS, 3rd") | ☐ Yes ☐ No |
|          | • "Scheduled Update" is enabled, and Last Update Date of Virus Pattern (Please refer to Section 8.7.1 - 2e of "Installation Guidelines for WebSAMS, 3rd") | ☐ Yes ☐ No |

| 3        | WebSAMS Router and School Internet Gateway | | |
| 3.1      | Configurations of WebSAMS Router and School Internet Gateway | (Please refer to "Doc. 16 - Rules for Configuration of WebSAMS Router and Internet Gateway") | ☐ Yes ☐ No |

| 4        | WebSAMS Workstation | | |
| 4.1      | Screen Saver Timeout is enabled with displaying Logon Screen on resume | ☐ Yes ☐ No |
| 4.2      | Anti-Virus Software | | |
|          | • Real-time Protection is enabled | ☐ Yes ☐ No |
|          | • Auto-update of virus definition is enabled, and Last Update Date of virus definition | ☐ Yes ☐ No |

| 5        | IT in ED workstation (if accessing WebSAMS) | | |
| 5.1      | Accessing WebSAMS Website with one ITED workstation, "https" is enabled | ☐ Yes ☐ No |
| 5.2      | Screen Saver Timeout is enabled with displaying Logon Screen on resume | ☐ Yes ☐ No |
| 5.3      | Anti-Virus Software | | |
|          | • Real-time Protection is enabled | ☐ Yes ☐ No |
|          | • Auto-update of virus definition is enabled, and Last Update Date of virus definition | ☐ Yes ☐ No |
System Security Setting Checklist for WebSAMS (cont'd)

To ensure system and data safety, schools are advised to:

- follow basic requirements as recommended in the WebSAMS Security Guide and Recommended Practice

- conduct the checking on a regular basis as well as a need basis

- properly keep the completed checklist for record purpose
  - (schools are NOT required to submit this checklist to the EDB)
System Security Setting Checklist for WebSAMS (cont'd)

For enquiries:

- Technical support:
  - WebSAMS Helpdesk 3125 8510

- Other enquiries:
  - School Liaison Officer of the WebSAMS Team
其他

相關網頁連結

- 網上校管系統簡介會
- 培訓行事曆網頁
- 教育局網上校管系統網頁
- 《香港增補字符集》(HKSCS)
- 香港教育城校管系統討論區
- 資訊科技教育
- 政府資訊科技總監辦公室 (OGCIO)
- 資訊安全網 (InfoSec)
- 香港電腦保安事故協調中心 (HKCERT)
教城討論區

WebSAMS 討論區

第1頁 / 共325頁 1 2 3 4 5 6 → 325 下一頁

STICKY THREADS

- SQL WebSAMS CDR內現特設【常用SQL參考庫】
  - nathanrd, 2012-11-14
  - 回覆: 4
  - 瀏覽: 633,982
  - 最後發表: 2013-01-16

- 討論區注意事項
  - edbeosim5, 2010-12-22
  - 回覆: 0
  - 瀏覽: 15,109
  - 最後發表: 2010-12-22

NORMAL THREADS
Q & A Section
The End