Bravura Privilege Implementation: Hardware Requirements for Session Monitoring

The session monitoring feature enables the monitoring, recording, searching, and viewing of actions performed during administrative sessions using *Bravura Privilege* credentials.

When configured, session monitoring works in the following way:

1. A self-service user logs in and requests privileged access via command prompt control or remote desktop control.
2. The user checks out access, triggering a monitoring session.
3. Recorded movie, image, or XML data files are stored on the *Hitachi ID Bravura Privilege* server.
4. Users with appropriate permissions can search files and download recorded sessions.

1 Session monitoring hardware requirements

Before calculating the hardware requirements for your organization, you should consider:

- What business drivers you have for recording sessions
- What login sessions should be recorded
- What type of data should be captured

1.1 Which login sessions should be recorded?

When deploying a session recording system, the first question is which sessions to record. There are several possibilities:

- All sessions, by all users
- All sessions to sensitive, but any user with access to those systems
- All sessions by high-risk users; that is, users whose actions could cause harm

The cost and impact of session recording technology directly affects how this question is answered. If capturing more sessions is relatively inexpensive and if it does not noticeably slow down the work of the affected users, then it makes sense to record more sessions. Conversely, as the cost of capture, transmission and storage rise, the motivation to more carefully target what is and what is not recorded rises.

In the context of session recording of system administrators, Hitachi ID Systems recommends that all logins to sensitive accounts should be recorded.

In the context of session recording of high-risk business users – for example, HR staff, financial trader – Hitachi ID Systems recommends that all logins by those users, to any system, should be recorded.

Over time, as the cost of storage and bandwidth continue to decline, it may make sense to record all login sessions by all users to all systems.

1.2 Determining required storage capacity

Storage capacity requirements can vary greatly depending on:

- Number of sessions recorded
- Type of data captured
- Frame rate used
- Session duration
- How often content is being updated on the screen
- Number of monitors used per session

Storage capacity requirements are also affected by the following session monitoring options:

- Color depth
- Capture video type
- Resolution / frame height/width / pixel density

1.3 What data should be captured

The data that can be recorded from a graphical user interface is extensive. It includes:

- Screen captures – image files of the contents of a single application or a user's graphical desktop
- Process information, such as the names of arguments passed to running program
- User interface elements, such as window titles, labels and text from input fields
- Keyboard events, such as key presses and releases
- Pointer device (mouse) events, such as movement and button clicks
- The contents of the operating system copy buffer
- Filesystem events, such as mounting or detaching network drives or removable media

- File transfers, such as copying files from one filesystem to another
- Video or image streams from a video capture device such as a webcam
- Network data transfers, such as emails or web pages.

At a minimum, when recording the login sessions of a user into an administrator-level account, it makes sense to capture what they typed and what the system displayed. This means video capture as well as capture of input from both the keyboard and copy buffer.

Regarding video capture, it may make sense to capture the user's entire desktop, so that in the event that the user downloaded a file with sensitive data to his computer, the recording will show what he then did with that file. For instance, if sensitive file was briefly examined – as would be normal in the context of troubleshooting – and then deleted, the action can be taken to be innocuous. On the other hand, if a sensitive file was copied to a USB flash drive or sent to the user's personal email account, the action can be interpreted as malicious.

Regarding input capture, it makes sense to capture both keyboard events and copy buffer contents. This is because the user may have constructed commands in advance and pasted them into the login session, without generating any keyboard events.

Finally, it may make sense to capture webcam video. This is useful in the event of serious misconduct leading to legal proceedings. When this happens, the user in question is likely to claim that the recorded actions were taken by someone else, that someone stole their access. Webcam capture will show who was performing those actions.

Note: Most corporate privacy regulations will prevent the use of webcam recording.

1.4 Screen capture trend analysis

Screen captures (including webcam captures), are the most intensive session recording both in terms of storage and network usage. For this reason, the following is an analysis of a variety of variables and how they affect the total storage and network usage.

Unless otherwise specified, ActiveX remote desktop disclosure is configured. Guacamole uses considerably less disk space, and is not directly analyzed here.

1.4.1 Resolution trend analysis

Resolution does not greatly affect the performance of sessions or their recordings.

The maximum dimension supported is 1280 x 720.

1.4.2 Color depth comparison

By default, sessions are recorded at 32-bit color depth. This can be reduced to 16-bit, and will reduce the raw disk space required by approximately 60%. The compressed disk space, however, will be only slightly

less than that of 32-bit.

1.4.3 Frame rate trend analysis

The frame rate directly affects how much storage is required. When the frame rate is doubled, that is, twice as many screenshots are taken per second, the storage required is roughly doubled as well.

1.4.4 Restricted scope comparison

When restricted scope is disabled, more than one monitor can be recorded per session. In this case, the storage is directly proportional to the increase area recorded.

The storage required is doubled when two monitors are recorded instead of one, assuming the same frame height and width for both monitors.

1.4.5 Concurrent session trend analysis

The amount of storage required is directly related to the number of sessions being recorded. Recording 100 sessions will require 10 times more storage than recording 10 sessions.

1.4.6 Usage trend

Storage required is strongly related to activity within a session. Activity can range from being idle (0%), that is, nothing on screen changes, to constant changes (100%), such as watching a video or running a living screen-saver.

The average user will likely use no more than 10-20%. However, since it is difficult to guess what is changing on a user's screen, a sample of routine sessions should be measured.

1.4.7 Case studies

Assuming the following:

- Default frame rate of 1/second
- Frame width x height of 1280 x 960
- Video capture
- RDP disclosure
- ActiveX

The following formula can be used to estimate the storage required for raw video:

```
S = N * (0.5 * A + 2.2)
```

where

S = Storage in MB/min

N = total sessions

A = percentage of screen activity

Forensic audits

In the event that an IT user is under suspicion or has been found to act unethically or illegally, it is helpful to be able to play back all of that user's activity, to see what inappropriate actions they may have taken. This data may be required as supporting evidence if the user must be terminated and may be needed in the course of legal proceedings thereafter. This data may also be needed to find and reverse any harmful changes the user has made to systems or data.

In this case, you may consider capturing video data for all IT staff only.

Assuming there are 100 staff in the IT department, and each runs one 8-hour session per day, with 10% screen activity, use the equation above to determine the storage required for 1 year:

```
S = N * (0.5 * A + 2.2) MB/min

 = 100 * (0.5 * 0.1 + 2.2) MB/min

 = 225 MB/min

 = 225 MB/min * 60 min/hr * 8 hr/day * 220 work days/year

 = 23760000 MB/year

 = 23760 GB/year
```

1.4.8 Load balancing considerations

It is recommended that you provision several load balancing replicated servers accessible by a single URL. Multiple replicated servers are required to carry the data load created by the monitored sessions and ensure a quality service. A single URL simplifies configuration and failover situations if a monitoring server needs to be taken down for maintenance or replaced.

Note that an end user needs to be able to access both the direct URL of the server and the load balanced URL in order to download packages containing video data. When the user attempts to download a session, *Hitachi ID Bravura Privilege* uses the direct URL (not the load balancing one) to trigger the downloading of the package to the user's workstation. This means that the user must be able to connect to the direct *Bravura Privilege* URL using their browser without it being blocked by a firewall.

See also:

- The *Bravura Security Fabric* Documentation for more information about session monitoring.