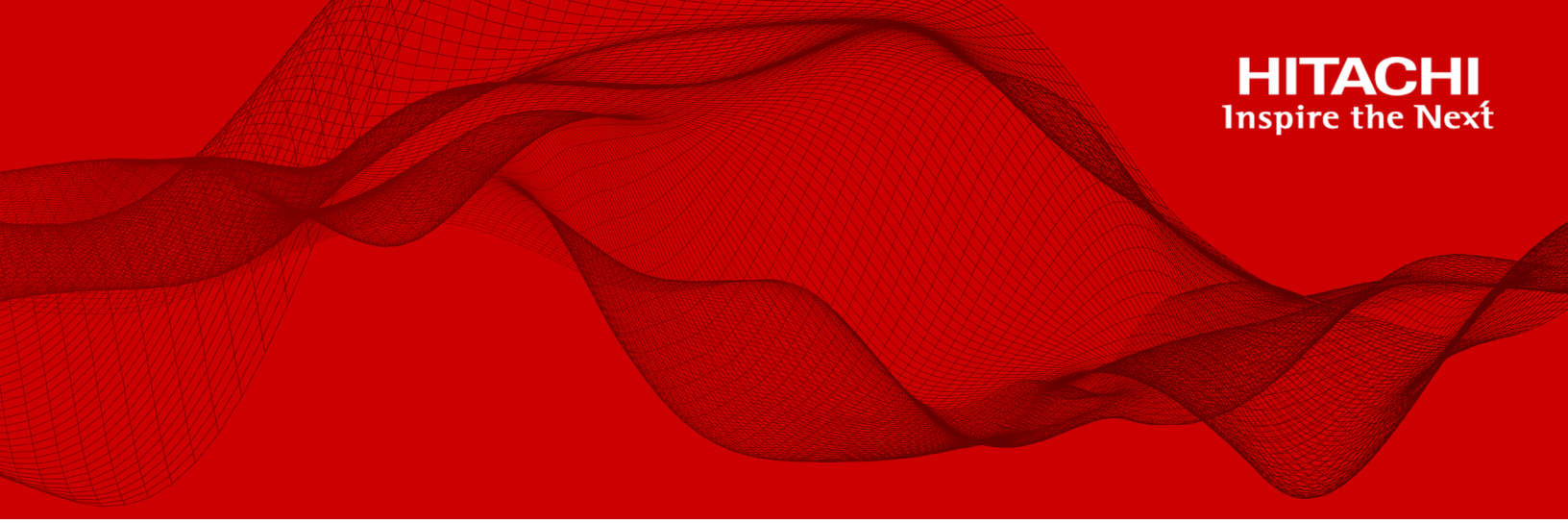

Locking down

a Bravura Security Fabric server

Organizations deploying *Hitachi ID Bravura Security Fabric* need to understand how to secure its runtime platform. *Bravura Security Fabric* is a sensitive part of an organization's IT infrastructure and consequently must be well defended.

This document is a best practices guide for securing a *Bravura Security Fabric* server. The objective of is to have a reliable, high availability platform that is difficult or impossible to compromise.

Contents

1 Introduction

Organizations that are either considering deployment of *Hitachi ID Bravura Security Fabric*, or have already deployed it, need to understand how to secure the *Bravura Security Fabric* server. *Bravura Security Fabric* is a sensitive part of an organization's IT infrastructure and consequently must be defended by strong security measures.

It is important to protect not only the *Bravura Security Fabric* server, but also the sensitive data it stores:

- Administrator credentials used by *Bravura Security Fabric* to connect to target systems.
- Console user passwords used by the *Bravura Security Fabric* administrator to sign into, configure and manage *Bravura Security Fabric* itself.
- Passwords to managed accounts on target systems.
- Password history and security question data for end users.

This document is organized as follows:

2 Basic precautions

Some of the most effective security measures are common sense:

- Use a single-purpose server for *Hitachi ID Bravura Security Fabric*. Sharing this server with other applications introduces more complexity and more administrators, each of which carries its own incremental risk.
- Use strong passwords for every administrative account on the server.
- Maintain a current, well-patched operating system on the *Bravura Security Fabric* server. This eliminates well-known bugs that have already been addressed by the vendor (Microsoft).
- Automatically apply patches, especially security patches, to the OS, database server and any third party software.
- Keep the *Bravura Security Fabric* server in a physically secure location.
- Provide security awareness training to all employees.
- Install and keep up to date anti-virus software.
- Do not leave a login session open and unattended on the *Bravura Security Fabric* server's console.
- If you are hosting *Bravura Security Fabric* on your own server, attach the server to a secure, internal network rather than the public Internet. If access from the Internet is required, mediate it via a reverse web proxy running a different OS an web server platform than *Bravura Security Fabric* – platform diversity reduces the risk of zero-day exploits. This is not an issue when using the software-as-a-service (SaaS) option.
- Regularly review *Bravura Security Fabric*, OS and network logs.
- Use the Microsoft Security Compliance Toolkit to learn more about server hardening.

3 Physical access and security

Hitachi ID Bravura Security Fabric servers should be physically protected, since logical security measures can often be bypassed by an intruder with physical access to the console:

- **Restrict physical access**

  Put *Bravura Security Fabric* server(s) in a locked and secured room. Restrict access to authorized personnel only. Product administrators should install and configure the server(s) and then only access it remotely via HTTPS to its web portal or RDP to the OS.

- **Connect a UPS**

  Ensure that server power is protected, that graceful shutdowns occur when power is interrupted and that there is surge protection at least on incoming power connections.

- **Prevent boot from removable media**

  Configure the server to boot from an internal drive and not from removable media.

Where the *Bravura Security Fabric* server is virtualized, apply the above controls to the hypervisor.

4 Employee training

Security policies are only as effective as user awareness and compliance. Security awareness training should include:

1. Building security including authorization for visitors and ID badges.
2. Password policies, regarding complexity, regular changes, non-reuse and not sharing passwords.
3. Social engineering and phishing attacks, to help users recognize when a person, malicious web site or email tries to trick them into disclosing access or other information.
4. The consequences of a security breach, including consequences to users who may have supported the breach through action or inaction.
5. Effective security practices relating to mobile devices, such as laptops, smart phones and tablets.
6. Not leaving endpoints signed on, unlocked and unattended.

5 Hardening the operating system

Hitachi ID Systems requires that *Hitachi ID Bravura Security Fabric* be installed on the latest Microsoft Windows Server operarating system. The first step in configuring a secure *Bravura Security Fabric* server is to harden its operating system. The following are suggestions on how to lock down the operating system.

5.1 Patches

Hitachi ID Systems recommends that organizations follow their standard operating patching processes to promptly download and install all vendor-supplied patches for the OS, DB and web server, as these often address security problems. There has never been, in Hitachi ID Systems experience, a compatibility problem with *Hitachi ID Bravura Security Fabric* caused by such automated patching.

5.2 Limit logins to only legitimate administrators

One way to limit the number of users who can access the *Hitachi ID Bravura Security Fabric* server is to remove it from any Windows domain. If the *Bravura Security Fabric* server is not a member of a domain, it reduces the risk of a security intrusion in the domain being leveraged to gain unauthorized access to the *Bravura Security Fabric* server.

- Remove unused accounts, leaving just `psadmin` – the *Bravura Security Fabric* service account.
- Create one administrator account to be used by the *Bravura Security Fabric* OS administrator to manage the server and set a strong password on this account.
- Disable the default administrator account.
- Remove any Guest or unused service accounts.
- Remove the terminal services user account TsInternetUser. This account is used by the Terminal Service Internet Connector License.

For any accounts that must remain, limit their access. At a minimum, block access by members of 'Everyone' to files and folders on the server.

5.3 Minimize running services

Disable any unused service. This eliminates potential sources of software bugs that could be exploited to violate the server's security. Only the following Windows services are required on *Hitachi ID Bravura Security Fabric* servers:

- Application Information
- Background Tasks Infrastructure Service
- DCOM Server Process Launcher

- DHCP Client
- Group Policy Client
- Local Session Manager
- Network Store Interface Service
- Power
- Remote Procedure Call (RPC)
- RPC Endpoint Mapper
- Security Accounts Manager
- SQL Server (MSSQLSERVER)
- System Events Broker
- Task Scheduler
- TCP/IP NetBIOS Helper
- User Profile Service
- Windows Process Activation Service
- Workstation
- World Wide Web Publishing Service

Additional services should only be enabled if there is a specific need for them.

5.4 Packet filtering

Open ports are an exploitable means of system entry. By limiting the number of open ports, you effectively reduce the number of potential entry points into the server. A server can be port scanned to identify available services.

Use packet filtering to block all inbound connections other than the following default ports required by *Hitachi ID Bravura Security Fabric*:

Default TCP port	Service
443/TCP	IIS / HTTPS web service.
5555/TCP	*Bravura Security Fabric* database service default port number (`iddb`).
2380/TCP	*Bravura Security Fabric* file replication service default port (`idfilerep`).
3334/TCP	Password manager service (`idpm`).
2340/TCP	Session monitoring package generation service (`idsmpg`).
2540/TCP	Discovery service (`iddiscover`).
6190/TCP	Privileged access service (`idarch`).
2240/TCP	Workflow Manager service (`idwfm`).
2234/TCP	Transaction monitor service (`idtm`).

6 IIS web server

The IIS web server is a required component since it provides all user interface modules. It should therefore be carefully protected, as described in the following subsections.

6.1 General guidelines

IIS is more than a web server; it is also an FTP server, indexing server, proxy for database applications and a server for active content and applications. Disable these features as *Hitachi ID Bravura Security Fabric* does not use them.

Always deploy a proper, issued-by-a-real-CA SSL certificate to *Bravura Security Fabric* servers and disable plaintext HTTP access. Never use a self-signed certificate in a user-facing system, as this may condition users to ignore SSL validity warnings.

Assign the IIS user the right to read from but not write to static HTML, image file and Javascript files used by *Bravura Security Fabric*.

Assign the IIS user the right to execute CGI programs but not other executables on the *Bravura Security Fabric* filesystem.

Disable directory browsing – there is no reason why a user connecting to the *Bravura Security Fabric* web portal should be able to list files in any folder.

7 SQL Server Database

Each *Hitachi ID Bravura Security Fabric* server is configured with a SQL Server database. Most commonly, the database server software is deployed on the same server as the *Bravura Security Fabric* application. It follows that the database must also be hardened.

7.1 Remove or disable unused services and components

Don't install anything beyond the core SQL server software. Specifically, leave out or disable:

- SQL Server Analysis Services (SSAS).
- SQL Server Integration Services (SSIS).
- Full-Text Engine.
- The Filter Daemon Launcher.
- SQL Server Reporting Services (SSRS).
- Active Directory Helper.
- SQL Server VSS Writer service.
- SQL Server Browser.

7.2 Disable TCP/IP access to MSSQL

Hitachi ID Bravura Security Fabric will connect to the database locally, so network access can and should be disabled. Use SQL Configuration manager to disable all but shared memory access to the database.

7.3 Limit access to the database

After installing the SQL Server database software and *Hitachi ID Bravura Security Fabric*, remove access by the OS Administrators group to the database and change the password for the sa account.

Configure a dedicated, local-admin account for use by The SQL Server Agent service, so that it runs in a different security context than the database itself.

8 Password and key management

During the installation of *Hitachi ID Bravura Security Fabric*, ensure that the security communication key (CommKey) used to encrypt communication between *Bravura Security Fabric* servers and other components on the network has been randomly created. Either create your own or use the default random key.

You should change the CommKey on a periodic basis. Note, the CommKey is located on all *Bravura Security Fabric* servers, secondary servers, proxy servers, and target systems using listeners (anything that calls the *Bravura Security Fabric* API). Identify all instances of the CommKey, schedule a change and complete the change, then test and verify that the change was successfully carried out.

Use a strong password policy for all passwords associated with the use of *Bravura Security Fabric*. At a minimum, always use the default password policy provided with *Bravura Security Fabric*.

9 Communication defenses

Hitachi ID Bravura Security Fabric sends and receives sensitive data over the network. Its communications include user passwords, administrator credentials, and personal user information.

9.1 HTTPS

Require HTTPS only connections to *Hitachi ID Bravura Security Fabric* and deploy real (i.e., not self-signed) SSL certificates on each server.

9.2 Firewalls

If you Internet access to *Hitachi ID Bravura Security Fabric* is required, protect this access using a firewall:

- Make sure you purchase all network hardware, including the firewall, directly from the manufacturer or from resellers who are authorized and certified by the equipment manufacturer.
- Always ensure the latest firmware running.
- Shutdown unused physical interfaces on the device.
- Implement access lists that only allow the protocols, ports and IP addresses required and deny everything else.
- Never use default usernames and/or passwords.
- Monitor outbound traffic to prevent internal machines from being used to launch a zombie attack on a server.
- Use egress filtering to block all traffic by default, then only allow certain traffic such as email and the Web.

- Consider purchasing a firewall which has three connections; one for the internal network, one for the Internet and the third for the DMZ.
- Use NTP to synchronize the time on the firewall. This will ensure the logs have the correct timestamps.
- Configure the Intrusion Detection System on the firewall if available.

9.3 Communicating with target systems

Avoid sending sensitive data as plaintext:

- Where possible ensure that communications are encrypted.

  For example, if you have an Oracle target system, the default setup for the Oracle client is to configure unencrypted communications with the Oracle database. Ensure that you configure encrypted communication.

- When communications cannot be encrypted, you can:
  - Use a proxy server to set up a secure channel with the primary server.
  - Not synchronize the accounts on that target system and ensure that administrative passwords are periodically rotated.

10 Auditing

Audit logs are an important measure to identify and analyze suspicious activity.

Since anyone with administrator access to the *Hitachi ID Bravura Security Fabric* server can alter or remove audit logs, arrange for periodic archive of audit logs to a different server that is managed by different administrators.

Bravura Security Fabric administrators with appropriate privileges can run operation reports.

As part of the *Bravura Security Fabric*, the Logging Service (idmlogsvc) manages logging sessions for a particular instance. It captures event messages from *Bravura Security Fabric* program execution, and writes them to the configured log file (**idmsuite.log** by default).

The Logging Service also has the ability to write to the Windows events logs. See the "*Bravura Security Fabric* Reference Manual" for further information.

Windows also provides various audit logs through the **`Event Viewer`**. And IIS provides configurable logging information with `W3C Extended Log File Format`.

Ensure you review the logs of your network devices, such as the firewall, on a regular basis.

Accurate logging requires an accurate time stamp. It is recommended that the server set its time using a reliable network time server.

An audit log is only effective if it is examined. Logs provide the best indications of break-ins, fraud and misuse. It is highly recommended that logs be examined on a regular basis.

11 Microsoft Security Compliance Toolkit

For environments that require added security, there are additional measures that can be taken to harden the servers. However, it is very important to conduct thorough testing in a test environment before implementing them in production.

Microsoft Security Compliance Toolkit has replaced all previous Microsoft security guides. Once installed you will have access to a myriad of guides and tools provided by Microsoft's security experts including:

- Windows Server Security Guides
- Microsoft recommended security baselines
- Tools to customize and export a security baseline for deployment

12 Further information

For further information on network security and server hardening refer to the following:

- The SANS Institute - An industry trusted organization that provides extensive collection of research documents in relation to information security.
- National Security Agency (NSA)
- National Institute of Standards and Technology (NIST)
- Internet Security Alliance (ISA) - information on industry best practices.
- The Center for Internet Security (CIS) - industry accepted hardening standards.
- International Organisation for Standardization (ISO) - industry accepted hardening standards.
- National Institute of Standards Technology (NIST) - industry accepted hardening standards.
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act 2002 (GLBA)

Note: The listed organizations provide information on computer security. Any mention of a commercial product is for informational purposes only and does not imply a recommendation or endorsement by Hitachi ID Systems.