Hitachi ID Bravura Security Fabric: Minimum Server Requirements

This document describes the minimum hardware specifications for a *Bravura Security Fabric* server.

1 Platform

Hitachi ID Bravura Security Fabric must be installed on a Windows Server, with Windows 2019 or Windows 2016 being recommended at the current release level of *Bravura Security Fabric*.

Installing on a Windows server allows *Bravura Security Fabric* to leverage client software for most types of target systems, which is available primarily on the "Wintel" platform. In turn, this makes it possible for *Bravura Security Fabric* to manage passwords and accounts on target systems without installing a server-side agent.

Each *Bravura Security Fabric* application server requires a web server. IIS is used as it comes with the Windows 2016 & Windows 2019 Server OS.

Bravura Security Fabric is a security application and should be locked down accordingly. Please refer to the Hitachi ID Systems document about hardening *Bravura Security Fabric* servers to learn how to do this. In short, most of the native Windows services can and should be removed, leaving a very small attack surface, with exactly one inbound TCP/IP port (443):

1. No ASP, JSP or PHP are used, so such code interpreters should be disabled.
2. Web-facing .NET is not used and should be disabled (some connectors require it, due to .NET API bindings).
3. No ODBC or DCOM are required inbound, so these services should be filtered or disabled at the web server. As with .NET, ODBC is sometimes needed to connect to target systems.
4. Inbound file sharing should be disabled.
5. Remote registry services should be disabled.
6. Inbound TCP/IP connections should be firewalled, allowing only port 443, remote desktop services (to configure the software) and a handful of ports between *Bravura Security Fabric* servers, mainly for data replication.

Each *Bravura Security Fabric* server requires a database instance. Microsoft SQL 2016 or 2019 are the recommended versions.

Bravura Security Fabric is compatible with 64-bit Windows Servers:

1. The core software is compiled as 64-bit binaries.

2. Components that execute in the context of the core OS, such as password synchronization triggers, event hooks, etc. are available in both 64- and 32-bit versions for compatibility.

2 Virtualization

Hitachi ID Bravura Security Fabric is compatible with VMware, Xen Project, Microsoft Hyper-V and Oracle VirtualBox virtual machine platforms. It can also be deployed on IaaS, including AWS. It generally works well with other virtualization platforms, but Hitachi ID Systems primarily tests with these. Hitachi ID Systems officially supports running *Bravura Security Fabric* on these virtual servers and will make a best effort to support customers who run on other hypervisors.

So long as the database server that hosts the *Bravura Security Fabric* back-end has access to reasonably fast I/O (e.g., NAS or similar) and so long as connectivity between the *Bravura Security Fabric* application sever and the database is fast and low latency (e.g., 1Gbps/1ms) there should is no adverse performance impact when comparing *Bravura Security Fabric* installed on hardware vs. *Bravura Security Fabric* installed on a similarly-equipped virtual server.

The key point above is to ensure sufficient I/O capacity for the database (MSSQL). If the database server is virtualized, using network attached storage (NAS) is recommended, as virtualized I/O (files such as VMDK's emulating an HDD image) is often substantially slower than physical I/O.

Even where customers choose to deploy the main *Bravura Security Fabric* servers on raw hardware, virtual machines are an excellent platform for proxy servers, test servers, development servers and model PCs.

A related question is often "how large can the deployment get before we have to move from a VM to hardware?" Unfortunately, there is no simple, universal answer:

1. Virtual servers vary in capabilities – they may have a 32-bit or a 64-bit CPU, may have 1, 2, 4 or 8 CPU cores allocated, may have different amounts of memory and may link to different types of storage infrastructure.

2. The load created by the application also varies – is there complex business logic? Do users access the application at random times or all at once? Are there just a few or thousands of integrations?

This variability means that the safest bet is to use benchmark results, using a configuration as similar as possible to the production setup, to gauge the performance of *Bravura Security Fabric* on representative physical and virtual servers.

3 Application server: hardware and OS

Production *Hitachi ID Bravura Security Fabric* application servers are normally configured as follows:

- Hardware requirements or equivalent VM capacity:
  - Intel Xeon or similar CPU. Multi-core CPUs are supported and leveraged. Dual core is a minimum.
  - At least 16GB RAM – 32GB or more is leveraged and is typical for a server.
  - At least 600GB of HD storage, preferably in an enterprise RAID configuration for reliability and preferably larger for retention of more historical and log data.

    More space is always better, to increase log retention.
  - At least one Gigabit Ethernet NIC.
- Operating system:
  - Windows Server 2019 (recommended) or 2016. Windows Server 2012 R2 is supported by Hitachi ID Systems but not recommended.
  - All available service packs and hotfixes should be applied (automatically).
  - It is recommended that the server is not a domain controller.
  - Core mode on Windows Server is supported.
- Installed and tested software on the server:
  - TCP/IP networking, with a static IP address and DNS name.
  - IIS web server with a valid SSL certificate and the following configured: CGI, HTTP redirect, URL Rewrite, and Dynamic Compression.
  - At least one web browser (i.e. Chrome) and PDF viewer.
  - Python 3.5.3 (64-bit).
  - A Git client (for revision control).
- A Microsoft SQL Server 2019 (recommended), 2016 or 2014 instance is required to host the *Bravura Security Fabric* schema:
  - Normally one database instance per application server.
  - The SQL Server database software can be deployed on the same server as the *Bravura Security Fabric* application, as this reduces hardware cost and allows application administrators full DBA access for troubleshooting and performance tuning purposes.
  - SQL Server 2019, 2016 or 2014 Standard is recommended in almost all cases – SQL Express is acceptable for small deployments and evaluations.

4 Database server: compatible software

Hitachi ID Bravura Security Fabric requires MS SQL Server 2019 or 2016, typically with one database instance per application server. In most environments, the Microsoft SQL Server software is installed on the same hardware or VM as the *Bravura Security Fabric* software, on each *Bravura Security Fabric* server node. This reduces hardware cost, eliminates network latency and reduces the security surface of the combined solution.

Be sure to install the following components that come with Microsoft SQL Server 2019 and 2016:

- Database Engine Services
- Client Tools Connectivity
- Management Tools - Basic
- Management Tools - Complete

Database I/O performance on a virtualized filesystem (e.g., VMDK or equivalent) is slow. If the database server software runs on a VM, please use a fast, nearby NAS or SAN to store the actual data files.

Bravura Security Fabric can leverage an existing database server cluster, but Hitachi ID Systems recommends a dedicated database server instance, preferably one per *Bravura Security Fabric* application server, installed on the same OS image as the core application.

1. The data managed by *Bravura Security Fabric* is extremely sensitive, so it is desirable to minimize the number of DBAs who can access it (despite use of encryption).
2. SQL Server has limited features to isolate workloads between database instances on the same server. This means that a burst of activity from *Bravura Security Fabric* (as happens during auto-discovery) would cause slow responses in other applications. Conversely, other applications experiencing high DB load would slow down *Bravura Security Fabric*.
3. *Bravura Security Fabric* already includes real-time, fault-tolerant, WAN-friendly, encrypted database replication between application nodes, each with its own back-end database. Use of an expensive DB server cluster is neither required nor beneficial.
4. Deploying the database to localhost has performance advantages (minimal packet latency from the application to its storage).
5. Allowing *Bravura Security Fabric* administrators full control over the database simplifies performance and related diagnostics and troubleshooting, especially when we consider that database administrators in most organizations are few in number and very busy.
6. Eliminating reliance on shared database infrastructure also eliminates the need to coordinate events such as database version upgrades, which involve reboots. Some Hitachi ID Systems customers who leverage a shared database infrastructure have experienced application disruption due to unscheduled and un-communicated database outages and restarts.

5 Deploying multiple servers

Hitachi ID Bravura Security Fabric supports multiple, load-balanced servers.

Each server can host multiple *Bravura Security Fabric* instances, each with its own users, target systems, features and policies.

Bravura Security Fabric instances can and normally do span multiple servers. Every server hosting a given instance is functionally identical. User traffic is load balanced between servers supporting the instance. Load balancing may be accomplished using DNS (round-robin is built into most DNS servers) or at the IP level with a device from Cisco, F5, etc.

High availability is accomplished by combining load balancing with server health monitoring and automatic fail-out. *Bravura Security Fabric* includes server monitoring tools that can be configured on each server to monitor its peers and when a failure is detected to trigger an alarm (e.g., by email) and to automatically update DDNS records to remove the failed server from circulation. Hitachi ID Systems also provides these tools for Unix/BIND with traditional DNS.

There is no coded limit to the number of concurrent, replicated servers. With more than 10 servers, replication may become slow. Since the three largest customers of Hitachi ID Systems run with just two production servers each, this is only a theoretical problem.

6 Using proxy servers to reach distant or firewalled systems

In some cases, the connection to a target system may be slow, insecure or blocked. This may be because the connection spans multiple data centers or uses an insecure network protocol.

To address such connectivity problems, *Hitachi ID Bravura Security Fabric* includes a connector proxy server. When a proxy server is deployed, the main *Bravura Security Fabric* server ceases to make direct connections to some target systems and instead forwards all communication to those systems through one or more connector proxies, which are co-located with the target systems in question.

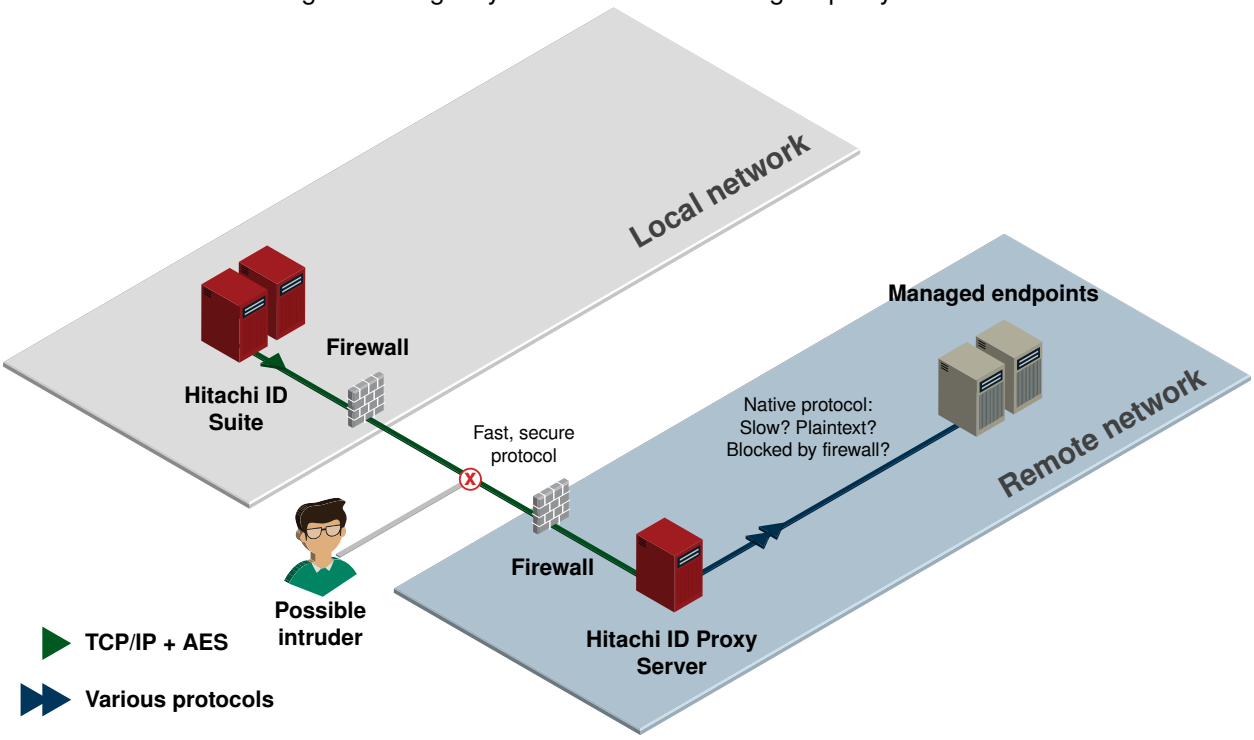
Communication from the main *Bravura Security Fabric* server to the connector proxy is encrypted and works well even when there is low bandwidth or high packet latency. It uses a single, arbitrarily-numbered TCP port number. Connections are established from the main *Bravura Security Fabric* application server to the proxy server. A single TCP port supports an arbitrarily large number of target systems at the connector proxy's location.

It is simple for firewall administrators to open a single TCP port per proxy server. Since connections are efficient and encrypted, there are usually no objections to doing so.

Communication between the proxy server and target systems continues to use whatever protocol each system supports natively. This communication is confined to a physically secure data center with a high-bandwidth, low-latency local network.

Deployment of the secure *Bravura Security Fabric* proxy server is illustrated in Figure 1.

Figure 1: Target systems connected through a proxy server



Hitachi ID Systems, Inc.
500, 1401 - 1 Street SE, Calgary AB Canada T2G 2J3 Tel: 1.403.233.0740 E-Mail: sales@hitachi-id.com