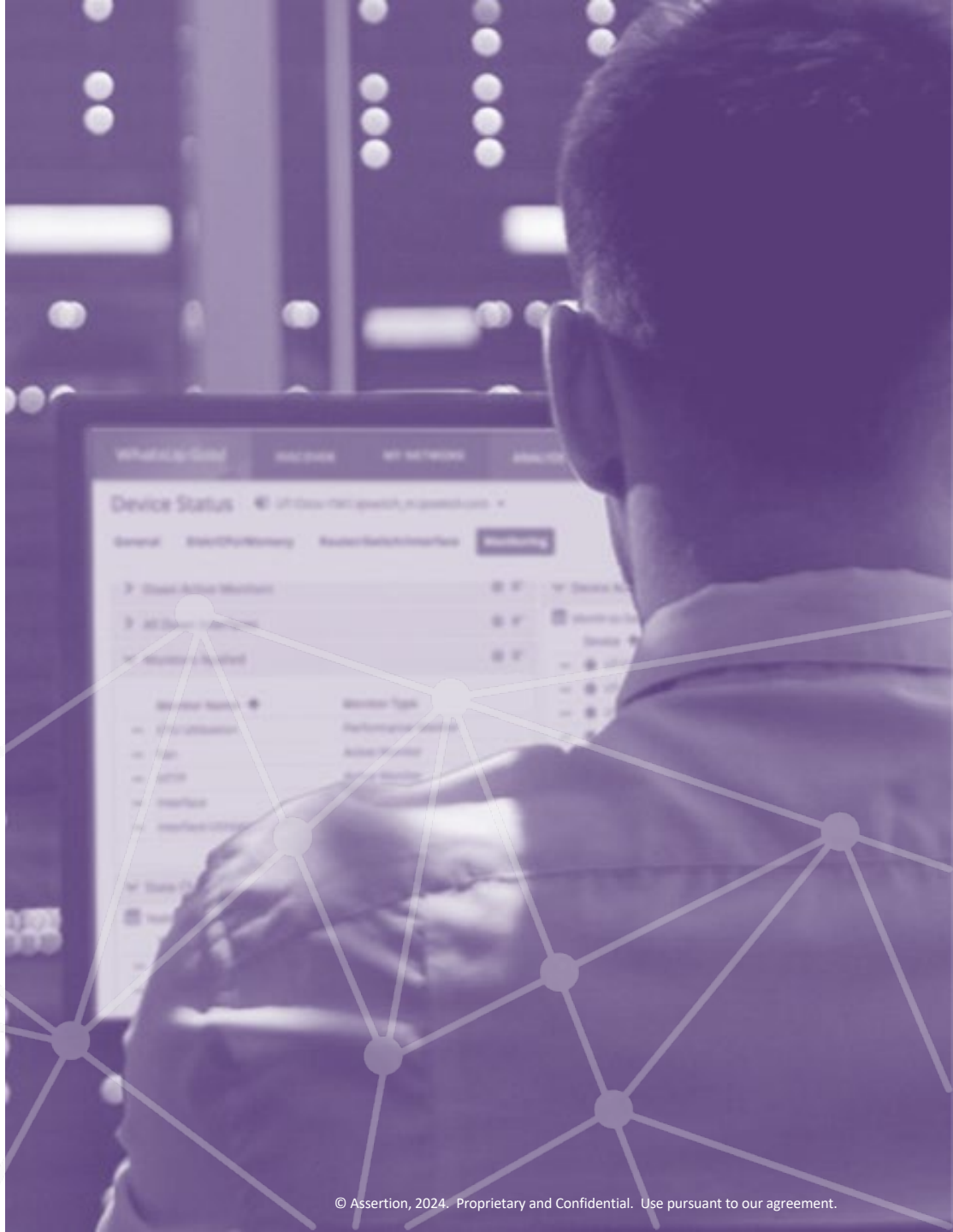
ASSERTION®
a voice security company

Smart Logging

Get real-time observability across all your voice assets in a single dashboard by proactively monitoring logs for issues. Go from issues to logs in 1-click. Detect errors, call & recording failures to improve service levels for managed services & cloud customers.

It integrates with 35+ voice products through Syslog for Linux and a custom log collector script for Windows.

July 2024



Index

Pain & Solution

Voice operations team has no visibility of issues until they impact services

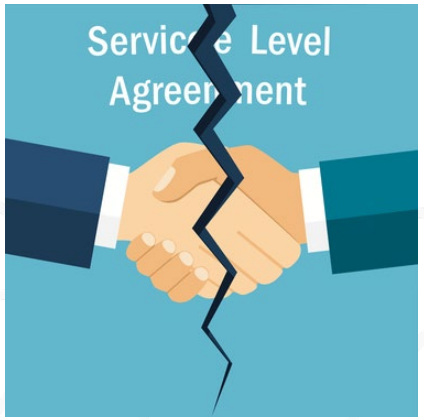
Existing monitoring systems lack timely visibility into critical issues like application errors, platform problems, system degradation, call failures, trunk downtime, and loss of recording. This delay in detection results in service disruptions, impacting business operations.

Proactively watch out for errors and budding problems and bring it to human attention

Logs from all voice systems are collected, scanned in near real time for errors and warnings when found, an alert is raised. Alert shows up on the dashboard, is notified via email and a ticket is raised for further processing.

Pain & Solution

Problems take too long to resolve and cause escalations and SLA violations



Challenges in accessing logs, such as access issues and missing logs, lead to delays in resolving escalations. These delays ultimately lead to breach of SLAs, impact the organization's ability to meet service level agreements effectively

When an incident happens, gather all the evidence in one place and have it ready for analysis

The portal provides 1-click access to logs directly from an event (alert). The engineer no longer needs to raise ticket to get credentials, spend time to login and gather all the logs, thus saving precious time that can be used to debug the problem.

Features

- Collect logs from 35+ voice systems without a log collection agent
- Vendor agnostic. Supports all major Voice vendors.
- Collect any log file – platform (OS) or application. Can add more files to pipe.
- Clone filters and forward logs for selective archival. Output in CEF, JSON and CSV to support all SIEMs.
- Single dashboard to monitor errors and system health
- 1-click access to logs from the web portal.
- Configure and manage simple log patterns on portal
- Detect complex patterns / correlate logs using workflows
- Custom dashboard widget for better observability
- Store local copy of logs for 30 days for immediate access
- Integrate with AD for authentication
- Get a report of alarms raised in last 30 and 365 days.
- Ability to transpose each log line into custom format
- Integration with ServiceNow for tickets.
- Rest API for downstream automation.

Benefits

1. Collect & process logs from 35+ voice products
2. Alert on Errors, Warnings and custom events
3. Clone, Filter and Forward logs
4. Maintain a local store of logs for up to 30 days
5. Go from event to evidence in 1-click
6. Detect operational issues like loss of logs, call failures etc.
7. Detect loss of recordings
8. Priced per data source monitored, billed monthly or annually

Smart Logging™ advantages over product native logging and alarming

Observability	Detect calls not maturing	Detect Trunk Down	Detect SIPRec failures on SBC	Report IAM changes & audit of local users
	Detect IVR & custom application failures	Detect user-defined patterns in logs	Collect logs from 35+ products + custom applications	Get alerts via dashboard, Email & REST API (tickets)
Health Check	Detect SBC down	Detect Loss of survivability (HA)	Detect Loss of Logs	Detect Asset health deterioration - CPU, Memory, Disk
Compliance	Detect loss of call recording*	Detect recording archival failures*	Mask PII in logs*	Track India OSP compliance*

*add on

Success Story

Airline

A top airline in Asia that operated an Avaya, Cisco, Oracle and Verint contact center products wanted to proactively monitor the systems for errors, warnings and custom events and be notified of the same in practically real-time. Since sensitive customers could be in the logs, they wanted to mask any such PII, if found.

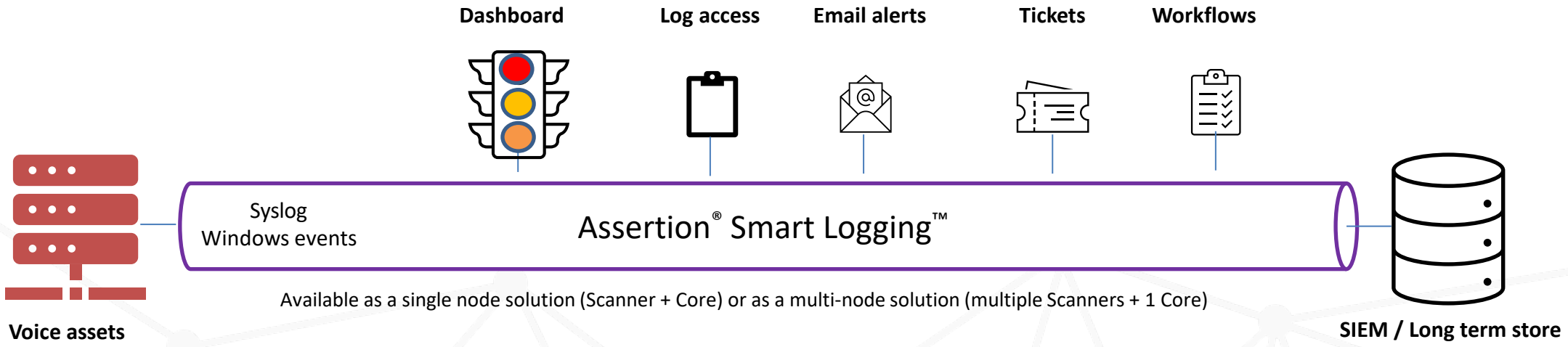
They implemented Assertion Smart Logging for 200+ voice servers, with near real-time log processing and alerts for errors, warnings, and custom events. The comprehensive dashboard improved network health visibility, while automated email alerts and ServiceNow tickets. The Voice Ops team gained quick access to 30 days of raw logs, significantly improving SLA adherence. PII masking ensured compliance with data privacy rules, and secured access via the bank's AD enhanced security.

Bank

A top 30 global bank operating in 60+ countries with a diverse voice network (Avaya, Cisco, AudioCodes, Oracle, Verint, and Microsoft Skype for Business) needed to collect logs from 800+ systems, filter IAM logs, and archive them separately for audit purposes. Not all products supported the Splunk HIDS agent, so collecting logs from every voice asset was not possible. Some systems could send logs to only one destination, so a method was needed to "clone" logs, archiving one copy in raw format and filtering another for IAM logs.

Assertion Smart Logging collated and collected logs from about 800+ voice servers from the bank. This agent-less system gathered logs from every voice system via various protocols and methods, cloning them into two copies. Raw logs were stored on a NAS, while filtered IAM logs were organized by product, asset, and date for easy retrieval. This streamlined log management and ensured compliance with audit requirements.

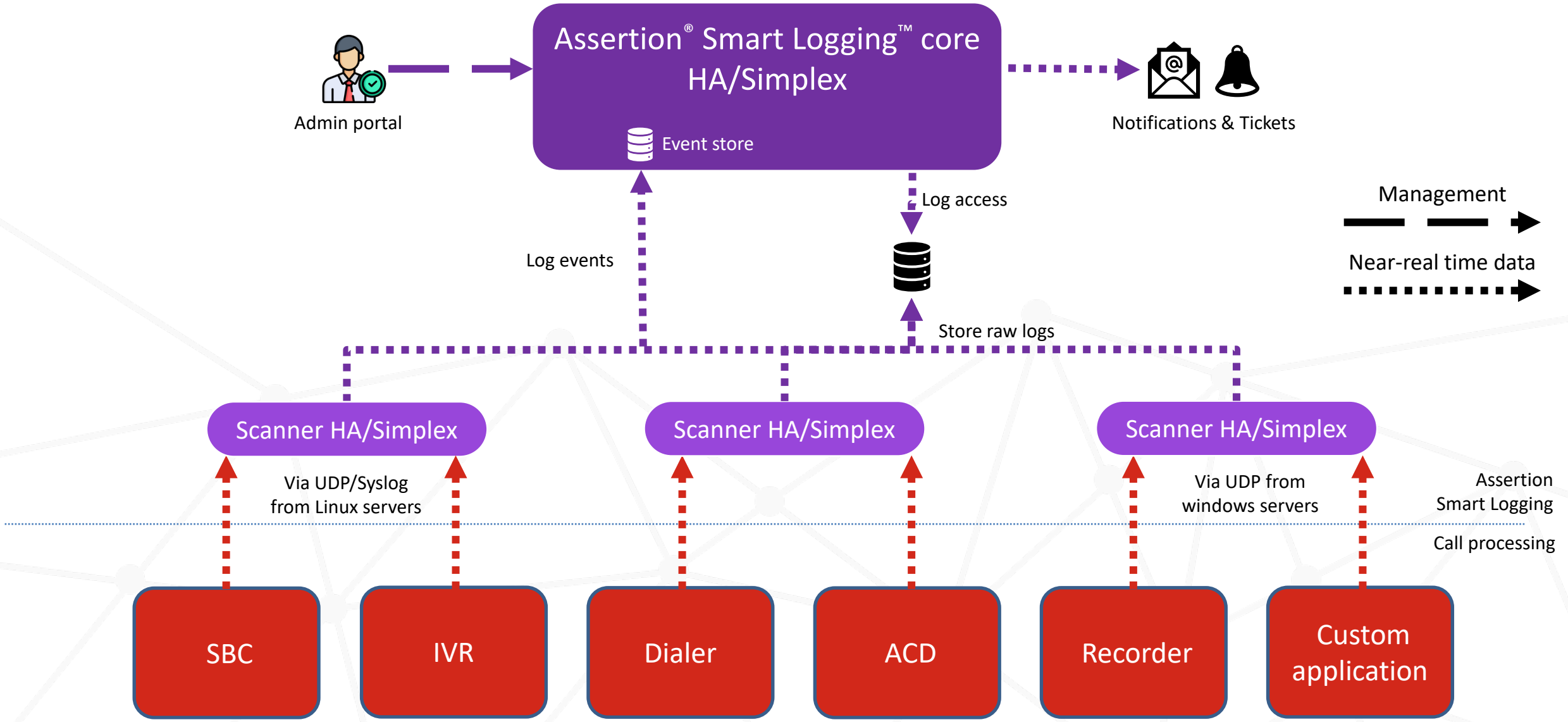
Assertion® Smart Logging™ is a pipe that collects, monitors and enables smarter archival of logs



NOTES:

- Access control via Enterprise AD / Local users
- Usually, the Scanner is connected to the management interface of the voice asset
- Out of the box integration supports detecting Critical and Major alarms from the log stream
- Custom single line patterns can be added via the self-service portal
- On Linux systems, custom data sources like log files can be ingested into the syslog stream by editing the syslog.conf file (will require sudo permission)
- On Windows systems, custom data sources like log files can be ingested into the log stream by editing the assertion's log transport script
- Custom workflows can be coded by Assertion for complex log pattern matching / correlation of logs across systems.
- Custom workflows can have UI widgets associated with them or a complete dashboard

Architecture Design - Proactive log monitoring with 1-click log access



Architectural considerations

- Assertion Smart Logging core supports geo-redundant HA
- Assertion Scanner supports active-standby HA in the same site
- Alarm is generated with either Smart Logging core or Scanner node fails
- There could be up to 10min processing delay in updating the dashboard after the Scanner receives the log.
- Each Scanner supports collecting logs from up to 50 systems. Multiple Scanners can be connected to the Core, without any known upper limit.
- Local storage will be for at least 7 days. There is no upper limit to the number of days the system can archive locally.
- Scanners can be “zoned” to handle assets in a certain geo to workaround network latency & regulatory requirements.

Product Screens

ASSERTION®

Dashboard

Select Date Range 02/Oct/2023 to 03/Oct/2023

See the alarms from all your critical voice infrastructure in one view

Events

SBCs 19

Core Infra 23

Recorders 12

Top-5 Assets with Events

10.33.55.124
10.59.76.21
10.77.32.168
10.29.98.212
10.87.163.82

Asset Health

Assets Down 5

Logs Archived

Understand the activity on your voice layer

Log Lines Archived 10.2 k

Bytes Archived 2.7 GB

Asset Status

02/Oct/2023 to 03/Oct/2023

Get a bird's eye view of health of all voice systems

Advanced Filter

IP Address	Asset Type	Category	Critical Events	Major Events	Custom Events
20.53.76.233	Oracle SBC	SBC	5	15	0
103.27.32.55	Avaya CM	Core Infra	3	7	2
103.33.41.25	Nice Recorder	Recorder	2	5	0

Click the event to get more details

ASSERTION®

Event Viewer

Select date range 04/Dec/2023 to 05/Dec/2023

Get a detailed view of each alarm

Advanced Filter

Severity	IP address	Asset Type	Category	Timestamp (UTC)	Detail	Logs
major	10.54.37.74	OSBC	SBC	05/Dec/2023 04:19:51	Dec 5 04:20:38 web2[b6d] ERROR Error: User admin login failed	Get logs ->
major	10.54.37.74	OSBC	SBC	05/Dec/2023 04:19:51	Dec 5 04:20:38 web2[b6d] ERROR AcliAuthCommAgent:: process_Response, Failed to authenticate	Get logs ->
major	10.54.37.79	AMS	Core Infra	05/Dec/2023 03:33:05	Dec 5 09:03:23 ams3779 sshd[26808]: error: PAM: Permission denied for cust from 192.168.252.193	Get logs ->
major	10.54.37.77	ACM	Core Infra	04/Dec/2023 14:44:50	Dec 4 07:45:42 localhost sshd[7349]: error: PAM: Permissio denied for dadmin from 192.168.252.186	Get logs ->
major	10.54.37.77	ACM	Core Infra	04/Dec/2023 14:44:47	Dec 4 07:45:39 localhost sshd[7349]: error: Could not l host key: /etc/ssh/ssh_host_dsa_key	Get logs ->
major	10.54.37.77	ACM	Core Infra	04/Dec/2023 14:41:48	Dec 4 07:42:40 localhost sshd[7189]: error: Could not load host	Get logs ->
major	10.54.37.77	ACM	Core Infra	04/Dec/2023 14:41:44	Dec 4 07:42:36 localhost sshd[7179]: error: PAM: Permission denied for dadmin from 192.168.252.186	Get logs ->

Click to get the detailed logs

ASSERTION®

Log Viewer

Select Duration 05/Dec/2023 2:46 PM (UTC) to 05/Dec/2023 3:01 PM (UTC)

Select Asset : 10.54.37.77

See the detailed logs on screen

Search Export

```
Dec 5 07:50:28 localhost sshd[29344]: error: Could not load host key: /etc/ssh/ssh_host_dsa_key
Dec 5 07:50:28 localhost pam_root_login[29347]: pam_root_login user name:dadmin
Dec 5 07:50:28 localhost pam_asg[29347]: Login for [dadmin] - rhost[10.54.37.176],tty[ssh]
Dec 5 07:50:28 localhost sshd[29344]: Accepted keyboard-interactive/pam for dadmin from 10.54.37.176 port 47250 ssh2
Dec 5 07:50:28 localhost sshd[29344]: pam_unix(sshd:session): session opened for user dadmin by (uid=0)
Dec 5 07:50:28 localhost sudo: dadmin : TTY=unknown ; PWD=/var/home/dadmin ; USER=root ; COMMAND=/opt/ecs/bin/defsat
Dec 5 07:50:28 localhost defsat: SAT_auth:session pid 29365 started from parent
Dec 5 07:50:29 localhost logmanager: SAT_auth:tui01: Login dadmin new session 29367 parent 29365
Dec 5 07:50:30 localhost root: cmSyslogConfig --iptcmquery
Dec 5 07:50:30 localhost logmanager: pam[2557]: Sid 0x10003c2a sat 2519 2001 dadmin dadmin 18 s 10.54.37.176 login
Dec 5 07:50:30 localhost logmanager: SAT_auth:tui01: Login dadmin Sid 0x10003c2a Pid 29367 Attempt 1 successful
Dec 5 07:50:30 localhost sudo: root : TTY=unknown ; PWD=/var/crash ; USER=root ; COMMAND=/opt/ecs/bin/customer_root_account status
```

Click to export the logs

Product Screens

Asset Health

Latest Log Received : >=60min ago X | Advanced Filter

Asset Name	IP Address	Asset Type	Category	Latest log received
Liverpool-SBC	20.53.76.233	Oracle SBC	SBC	2 hrs 15 min ago
Singapore-ACM1	103.27.32.55	Avaya CM	Core Infra	3 days 2 hrs 1 min ago
Singapore-Recorder1	103.33.41.25	Vering i360	Recorder	1 hr 3 min ago

Ensure logs are received continuously.
Get notified if logs are not received from an asset

ASSERTION® Recording Failures Dashboard

Select Date Range 19/Jan/2024 to 20/Jan/2024

Active and Passive recording failures.
Voice as well as digital failures

Recordings Failures
- 251 Passive Voice Recording Failures
- 87 SIPREC Voice Recording Failures
- 143 ACD Active Voice Recording Failures
- 115 Screen Recording Failures
- 29,134 Successful Recordings

Recordings Live — 39 Ongoing Sessions

Archival Failure Duration — 96+ hrs: 300 (9.53%); 72 - 96h: 484 (15.38%); 48 - 72h: 580 (18.43%); 24 - 48h: 735 (23.36%); 12 - 24h: 1048 (33.3%)

Top-10 Recorders with failures

Archival failures

ASSERTION® OSP Center Compliance Dashboard

Hey Admin

Select Date Range 19/Jan/2024 to 20/Jan/2024

CDRs — Avaya CM 75,338 | Oracle SBC 61,954 | Genesys PureCloud 69,223

Asset OSP Compliance Status

Asset	IP Address	CDR Oldest	CDR Latest	Oldest Log	Latest Log	Compliance
Avaya CM	10.55.32.107	1 Jan 2023 01:00	2 Feb 2024 15:00	1 Jan 2023 00:05	2 Feb 2024 15:21	✓
Oracle SBC	10.55.32.155	15 Jul 2023 01:00	2 Feb 2024 15:00	1 Jan 2023 00:03	2 Feb 2024 15:21	✗
Genesys PureCloud	-	1 Jan 2023 01:00	2 Feb 2024 15:00	-		✓

Be aware of your OSP Compliance status in an instant

Storage Disk Usage & Availability — Genesys PureCloud CDR (25 GB, 7.18%); ACM System Log (88 GB, 25.29%); Oracle SBC CDR (62 GB, 17.82%); ACM CDR (37 GB, 10.63%); Available Disk Sopace (136 GB, 39.08%)

Access Audit

Timestamp	Login ID	Role	Access Mode
19 Jan 2024 11:23	Pradeep	DPO	Full Access
7 Jan 2024 15:47	Sanjay	Operations	Masked
2 Jan 2024 12:22	Sanjay	Operations	Masked
19 Dec 2023 14:11	Pradeep	DPO	Full Access
11 Dec 2023 10:09	Sanjay	Operations	Masked
29 Nov 2023 16:44	Sanjay	Operations	Masked
23 Nov 2023 09:16	Pradeep	DPO	Full Access

ASSERTION® Settings

← Settings / Log Management / Masking

Advanced Filter | Asset Type : ACM X | Add | Apply Changes

Tag	Masking Pattern	Asset Type	Action
Telephone-number	\s\d{10}\s	Avaya Communication Manager	
Visa-Mastercard-number	\s(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14})\s	Avaya Communication Manager	

Configure masking rules to detect PII and replace it with 'xxxx' in the logs.
Multiple rules can be configured per asset type.
Logs from all assets including custom application logs and agent desktop logs can be masked.

Out-of-the-box support for major OEM voice systems

ASSERTION®

Asset Inventory

Add Asset | All Assets

*Latest major versions are supported

- AudioCodes One Voice Operations Center (ACOVOC)
- AudioCodes Session Border Controller (ACSBC)
- Avaya Aura Appliance Virtualization Platform (AVP)
- Avaya Aura Application Enablement Services (AES)
- Avaya Aura Communication Manager (ACM)
- Avaya Aura Device Services (AADS)
- Avaya Aura Experience Portal (AEP)
- Avaya Aura Media Server (AMS)
- Avaya Aura Messaging (AAM)
- Avaya Aura Session Manager (ASM)
- Avaya Aura System Manager (ASMGR)
- Avaya Aura Utility Services (AUS)
- Avaya Breeze (ABRZ)
- Avaya Call Management System (ACMS)
- Avaya Contact Recorder Advanced 15.x (ACR)
- Avaya Experience Portal EPM (AEP-EPM)
- Avaya Experience Portal MPP (AEP-MPP)
- Avaya Media Gateway G450 (AMG)
- Avaya Session Border Controller (ASBC)
- Avaya Social Media Hub (ASMH)
- Genesys Administrator (GEADM)
- Genesys Engage SIP Server (GESIP)
- Genesys ICON Server (GEICON)
- Genesys Infomart (GEINFO)
- Genesys Media Control Platform (GEMCP)
- Genesys Orchestration Server (GEORS)
- Genesys Pulse Server (GEPULSE)
- Genesys Resource Manager (GERM)
- Genesys Stat Server (GESTAT)
- Genesys Universal Routing Server (GEURS)
- Microsoft Skype for Business (SFB)
- Nice Engage Recorder (NICEREC)
- Oracle Enterprise Session Border Controller (OSBC)
- Verint Impact 360 (VI360)
- Verint Verba (VFC)

Hardware, Software and Network requirements

- Minimum 1 VMs - 1 Smart Logging Core to support 50 assets.
  - Add Scanners to support more assets, a scanner per 50 assets.
- Assertion® Scanner has the following requirements:
  - Hardware requirements – VM with 8GB RAM, 4 vCPU * 2.2GHz, free disk space of 150 GB.
  - Software requirements – OVA provided with RHEL 9.x. Customer to provide license.
  - Network – 2 NIC cards, 1Gbps
- Assertion® Smart Logging Core has the following requirements:
  - Hardware requirements – VM with 16GB RAM, 4 vCPU * 2.2GHz, free disk space of 500 GB.
  - Software requirements – OVA provided with RHEL 9.x. Customer to provide license.
  - Network – 2 NIC cards, 1Gbps
- Network attached SAN store – 5 TB
  - If SAN store is not available, the core will double up as log store. In that case, the core's disk requirement changes to 5 TB.

PoC / Trial offer

We offer a 30-day Proof of Concept (PoC) for Assertion Smart Logging tailored to meet your business needs!

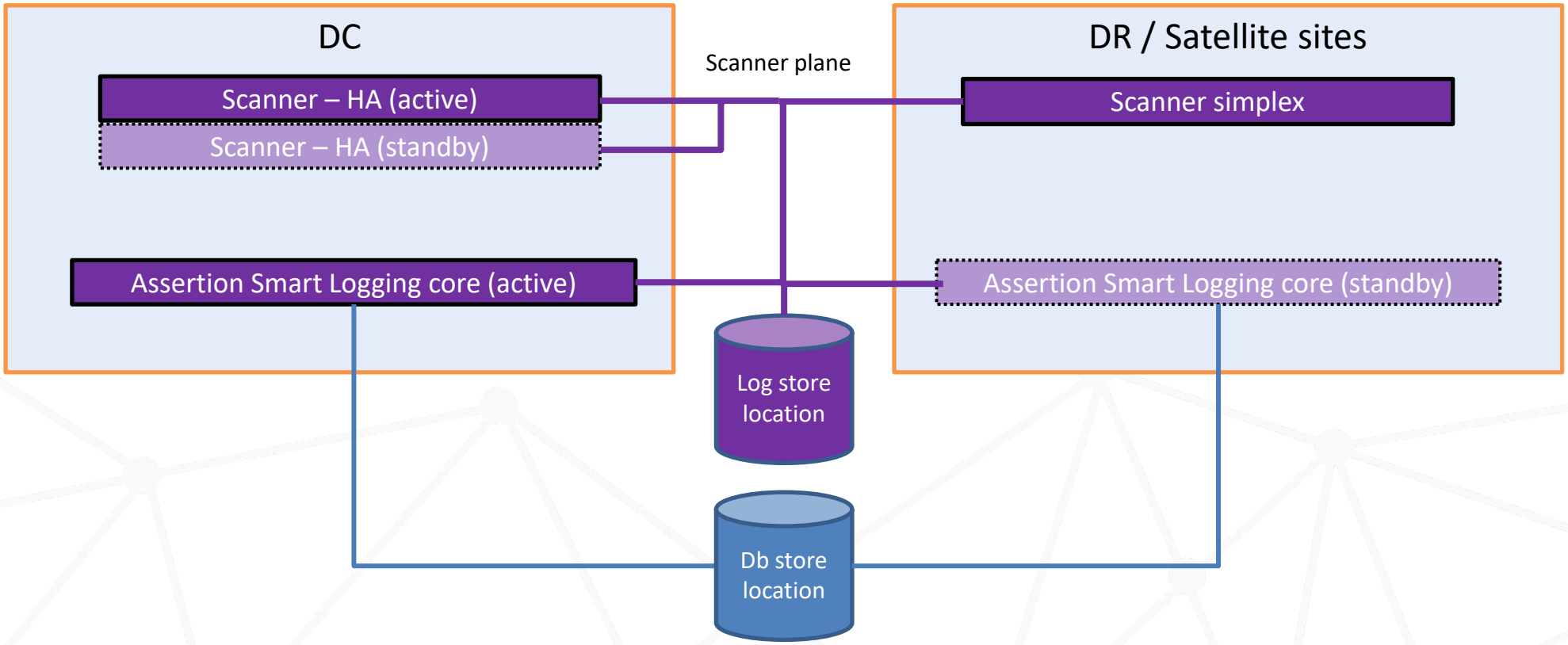
Opt for a no obligation PoC to test the system in your environment. Purchase only if the PoC is successful. This flexible approach allows you to experience the value of Assertion Smart Logging with confidence.

ASSERTION®
a voice security company

Thank you

Contact us today to discover how Assertion's innovative solutions can elevate your technology infrastructure and meet your evolving needs.

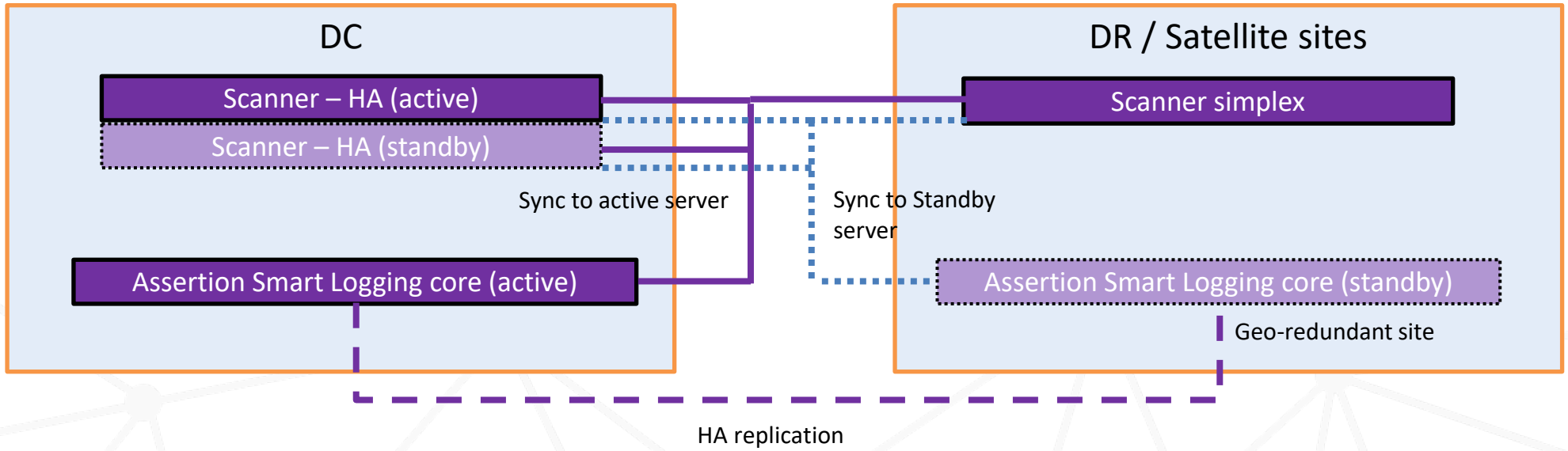
Smart Logging HA architecture



NOTE:

1. Scanner and Core independently reach the Log store.
2. Scanner will store the logs on local disk if it cannot reach the log store. It will upload to log store once connectivity is restored.
3. If connectivity between Scanner and Core breaks, an email alert will be triggered.
4. Scanner failover and failback in HA mode is automatic and transparent.
5. Core failover to standby and failback must be triggered manually.
6. Scanner will automatically reach the standby core server if active is not reachable.
7. The log store and Db store SAN locations must be highly available (pre-requisite).

Smart Logging special HA architecture



NOTE:

1. Scanner will uplink the logs to both Active and Standby Core servers simultaneously, at all times.
2. Core Active and Standby HA pair can be geo-separated. The replication is an on-going activity, at all times.
3. Core failover to standby and failback must be triggered manually.
4. Scanner will store the logs on local disk if it cannot reach the Core servers. It will upload to the Core server(s) once connectivity is restored.
5. If connectivity between Scanner and Core breaks, an email alert will be triggered.
6. Scanner HA nodes need to be co-located. Failover and failback in HA mode is automatic and transparent.