Valley Coastal Bend (VCB) Traffic Analysis

Valley Coastal Bend (VCB) VistA is one of two VistA's now housed in the AWS portion of VA's Enterprise Cloud (VAEC). In the *VistA Adaptive Maintenance Project* (VAM), AWS's traffic mirroring facility was used to copy the traffic of this VistA's Remote Procedure Call (RPC) interface. The RPC Interface is the main way VistA clients access the system.

Specifically the four gateways used by VistA clients to access VCB VistA were mirrored between 1/1/2020 and 1/19/2020 ("Monitored Period") and their traffic was combined for analysis. A similar approach would enable traffic analysis of any VistA housed in the VAEC.

In this analysis, connections to VistA are called *"Sessions"*. There are two types - those where a user signs into VistA ("Signon Sessions (SO)") and those where traffic may be sent between a client and VistA but a user doesn't sign on ("No Signon Sessions (NSO)"). Without a sign on, nothing of significance happens but there is overhead on the system.

In the monitored period, while *Signon Sessions* dominated traffic, a greater number of *No Signon Sessions* were created.

Type	Traffic	Sessions
Signon Sessions (SO)	**50.96 GB (95.47%)**	231,690 (42.02%)
No Signon Sessions (NSO)	2.42 GB (4.53%)	**319,748 (57.98%)**

In the following sections, the nature of both session types are examined in detail. The final section of the document makes recommendations based on this analysis with a focus on how to improve the security of the VistA system.

1. No Signon Sessions (NSO)

In the monitored period, **57.98%** of sessions made to this VistA did not sign on to the system. The median number of such sessions on a weekday, **18,560** is not far from the median for weekend days, **13,633**, a proportion not matched in Signed On sessions where weekdays dominate.

Besides a small number that [1] run through a basic RPC sequence to connect and exit and [2] a special message used by the *BSE* signon mechanism, these sessions check that VistA is still operating. This may be the legacy of when VistA's health wasn't actively managed, forcing applications and remote locations to actively monitor connectivity. This behavior persists even though VistA is now actively managed, making the majority of sessions to VistA wasteful **health checks** on the system.

Four classes of "health check" session can be identified from traffic patterns:

- send an older version of the RPC Protocol's connect message. These sessions come from VCB itself using VCB's 10.141 IP range. Sessions are created in every hour of the day with greater rates in the middle of the day during weekdays.
- come from one Austin Automation Center (AAC) address, 10.224.73.235, contain a basic set of RPCs that don't require a sign on and last for three minutes. They are dispatched evenly over 24 hours.
- have *no traffic* - a connection is opened and closed. They are created at a steady rate per hour, 24 hours a day and come from [a] a pool of IPs starting with *10.245.196* and [b] an AAC IP, *10.224.75.67*.
- contain unicode, non print characters, come from 10.224.75.67, the same AAC address of *no traffic* sessions and are also created at a steady rate per hour, 24 hours a day

2. Signon Sessions (SO) Overview

Signon Sessions represented **42.02%** of sessions seen in the monitored period and carried **95.47%** of the traffic.

Unless unofficial backdoors are utilized, a client must sign a user into a VistA to interact effectively with the system. VistA supports four different mechanisms for sign on, each with a "level of assurance".

> Four levels of assurance were outlined by a 2006 document from the National Institute of Standards and Technology (NIST). The level of assurance (LOA) is measured by the strength and rigor of the identity proofing process, the strength of the token used to authenticate the identity claim, and the management processes the identity provider applies to it.

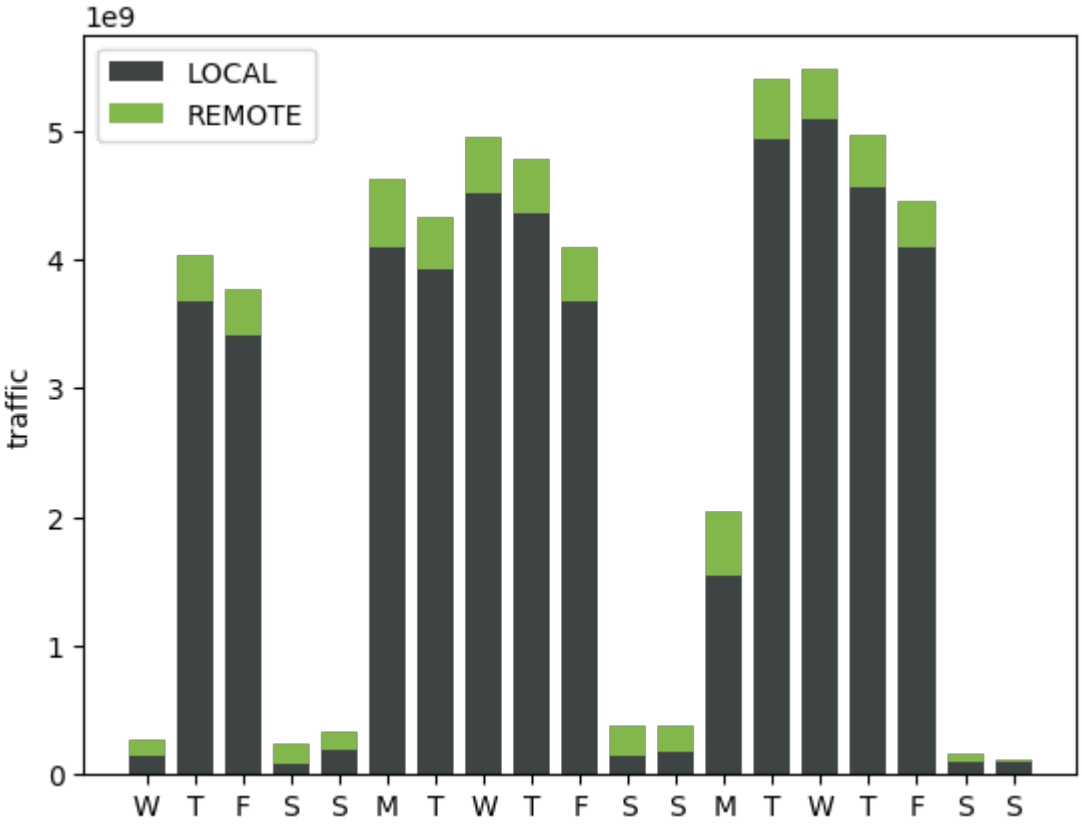
VistA's sign-on mechanisms are

Method	Level of Assurance	Description
CAPRI	1	an "honor system" where a client declares the identity of its user and VistA accepts those identifiers without checking any further. A record is automatically created for a user who doesn't already exist in a VistA.
Access Verify	2	a user record must exist in the VistA and two encrypted "passcodes", access and verify, identify and verify a user
BSE	2	a client first logs a user into their home VistA and obtains a security token. It then passes an encrypted form of that token along with a client identifier and user identifier to the target VistA. The target VistA calls back to the home VistA to validate that the token is valid. If it is, then the home VistA returns fuller user demographics and, as in CAPRI, the target VistA uses those demographics to create a user record if none exists.
PIV	3	Personal Identity Verification - a card leads to user and client credentials being sent to a VistA. As with Access-Verify, a user must already exist in the VistA.

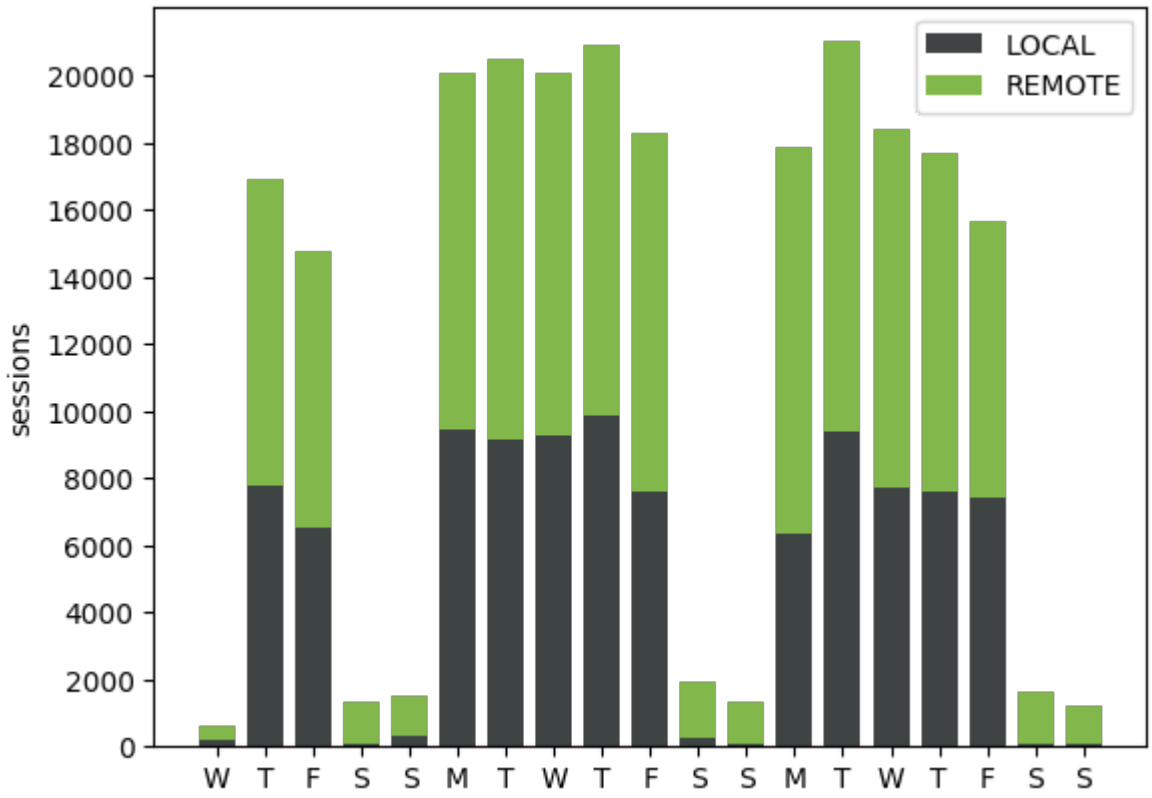
LOA 2 and 3 mechanisms account for roughly equal traffic during the monitored period but LOA 1, used by JLV, accounts for the majority of sign on sessions.

Type	Traffic	Sessions
LOA3	20.71 GB (43.68%)	18,604 (8.03%)
LOA2	20.58 GB (43.4%)	57,416 (24.78%)
LOA1	6.12 GB (12.92%)	155,670 (67.19%)

Another key breakdown of Signon Sessions is whether their users belong to the VistA being accessed ("Local Users") or their users are remote and belong to a different VistA ("Remote Users"). Most traffic for the monitored period was from local users.



but a slight majority of sessions were from remote users.



3. Local Signon Sessions

Local Signons describes the activity of end users who have VCB as their "Home VistA". Such users would have been formally added to VCB VistA by a human administrator and given specific permissions. Specifically it covers …

> activity by identified end users who [1] employ PIV or Access Verify to log on to *VCB* VistA or [2] whose JLV login specifies that they belong to *VCB* VistA ("JLV Local Users"). *Local* also covers activity by these users with *VRAM*, a BSE-based application most of whose activity is covered in the *Remote section* below.

This Local activity dominates signed-on traffic (**45.41 GB (89.1%)**) but accounts for less signed-on sessions (**99,255 (42.84%)**) than Remote activity. The median daily count of Local users (**790/35** [Weekday/Weekend]) also trails the median daily count of Remote users (**991/82** [Weekday/Weekend]).

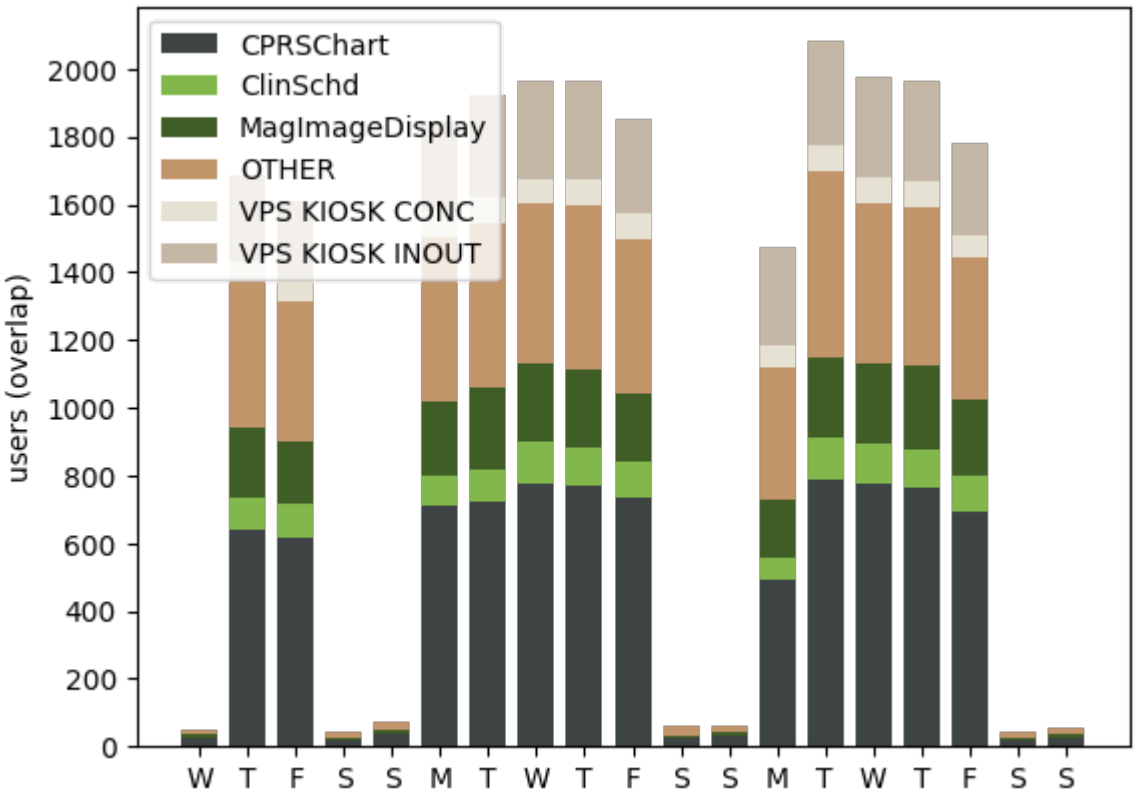
49 types of client were employed by local users during the monitored period. The following table is ordered by client traffic use. Clients are named with the labels used in PIVs and BSE. Notice how:

- CPRS's RPC and Traffic percentage were similar while JLV had much more traffic than its RPC count would suggest and many many more sessions - JLV alone was responsible for **47.9%** of the sessions employed by local users.
- VistA Imaging Display (MagImageDisplay) had many more daily users than its traffic implies. This is because most of its traffic was not RPCs. It was pulling images separately from VistA Imaging.
- User numbers dropped off precipitously on weekends - the first user number below shows the median number of weekday users, the second shows the median number for weekend days. *TRMPlus* is the one exception.

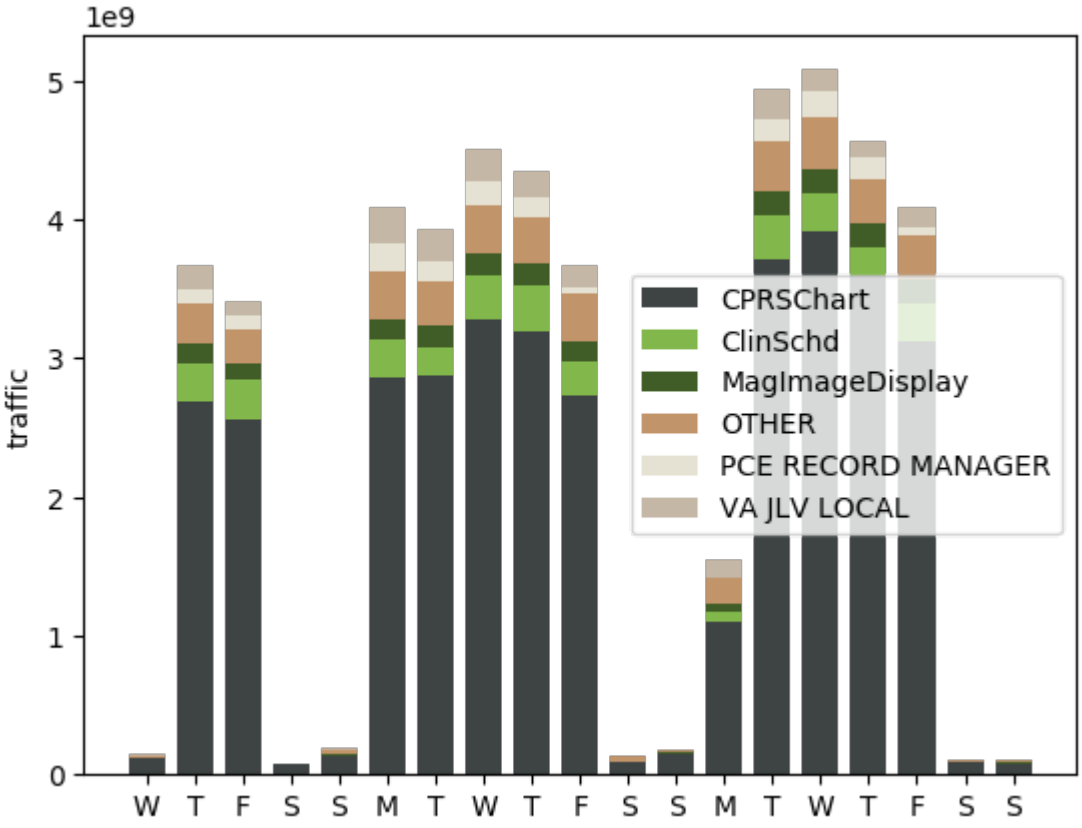
#	Name	Users (W/E)	Traffic	Sessions	RPCs
1	**CPRSChart**	724/25	33.88 GB (74.6%)	19,610 (19.76%)	43,020,128 (77.65%)
2	**ClinSchd**	107/0	2.84 GB (6.26%)	2,102 (2.12%)	4,220,510 (7.62%)
3	**VA JLV LOCAL**	62/1	1.99 GB (4.37%)	47,545 (47.9%)	505,235 (0.91%)
4	**MagImageDisplay**	220/7	1.72 GB (3.78%)	4,836 (4.87%)	800,949 (1.45%)
5	**PCE RECORD MANAGER**	3/0	1.36 GB (2.99%)	43 (0.04%)	820,966 (1.48%)
6	**ICB**	51/0	732.89 MB (1.58%)	918 (0.92%)	2,483,035 (4.48%)
7	**AuditReportManager**	7/0	577.78 MB (1.24%)	135 (0.14%)	1,386,583 (2.5%)
8	**FBCSDistributionProcessing**	24/2	479.57 MB (1.03%)	402 (0.41%)	105,592 (0.19%)
9	MagImageCapture	24/0	291.05 MB	428 (0.43%)	328,005 (0.59%)
10	dssroi	3/0	270.43 MB	38 (0.04%)	132,543 (0.24%)
11	FBCSAuthorization	19/2	224.59 MB	281 (0.28%)	164,010 (0.3%)
12	DSSAPAT	9/0	196.53 MB	178 (0.18%)	134,353 (0.24%)
13	YS MHA	47/0	177.92 MB	749 (0.75%)	238,275 (0.43%)
14	dentalmrmtx	9/0	172.04 MB	170 (0.17%)	258,780 (0.47%)
15	fbcspayment	9/1	136.81 MB	133 (0.13%)	147,224 (0.27%)
16	VPS KIOSK CONC	73/0	120.68 MB	7,410 (7.47%)	223,628 (0.4%)
17	PCERecordManager		81.59 MB	4	46,687 (0.08%)
18	AVAMBIG	8/0	72.83 MB	122 (0.12%)	39,361 (0.07%)
19	AbovePAR	2/0	58.1 MB	44 (0.04%)	25,104 (0.05%)
20	MHSuite	12/0	33.8 MB	138 (0.14%)	85,540 (0.15%)
21	VIAB	66/0	17.38 MB	3,213 (3.24%)	22,489 (0.04%)
22	ECS GUI	5/0	14.23 MB	160 (0.16%)	22,013 (0.04%)
23	TRMPlus	8/6	13.61 MB	166 (0.17%)	81,857 (0.15%)
24	BHL	6/0	8.8 MB	109 (0.11%)	17,161 (0.03%)
25	CW MAIL	3/0	8.44 MB	37 (0.04%)	8,326 (0.02%)
26	AntiCoagulate	2/0	6.25 MB	231 (0.23%)	10,449 (0.02%)
27	VPS KIOSK INOUT	286/1	5.14 MB	8,361 (8.42%)	41,872 (0.08%)
28	ACKQROES3E		2.21 MB	37 (0.04%)	2,363
29	*OTHER*		2.17 MB	2	1,646
30	ProsMenu	1/0	1.5 MB	20 (0.02%)	3,049 (0.01%)
31	ROES	4/0	1.11 MB	404 (0.41%)	5,375 (0.01%)
32	GroupNotes		1.0 MB	8 (0.01%)	796
33	PROSTHETICS		1021.96 KB	3	748
34	groupnotes		927.69 KB	2	580
35	BSETOKENGET	64/2	908.87 KB	1,090 (1.1%)	8,720 (0.02%)
36	VistARad		892.93 KB	4	376
37	VRAM	5/0	627.87 KB	81 (0.08%)	2,703
38	TRMCallLogReporter	1/0	551.51 KB	12 (0.01%)	372
39	VIPDirector		530.02 KB	2	1,709

#	Name	Users (W/E)	Traffic	Sessions	RPCs
40	CARD LOG REPORTER		255.89 KB	7 (0.01%)	240
41	Admin Management Console		132.84 KB	1	628
42	APATAdminTool		98.19 KB	3	290
43	ASISTS		89.52 KB	2	50
44	HUMAN RESOURCES		59.31 KB	3	127
45	FIM		50.21 KB	4	36
46	BCMA		33.57 KB	2	110
47	VitalsManager		25.26 KB	2	20
48	Vitals		25.1 KB	2	20
49	BCMApar		13.23 KB	1	14

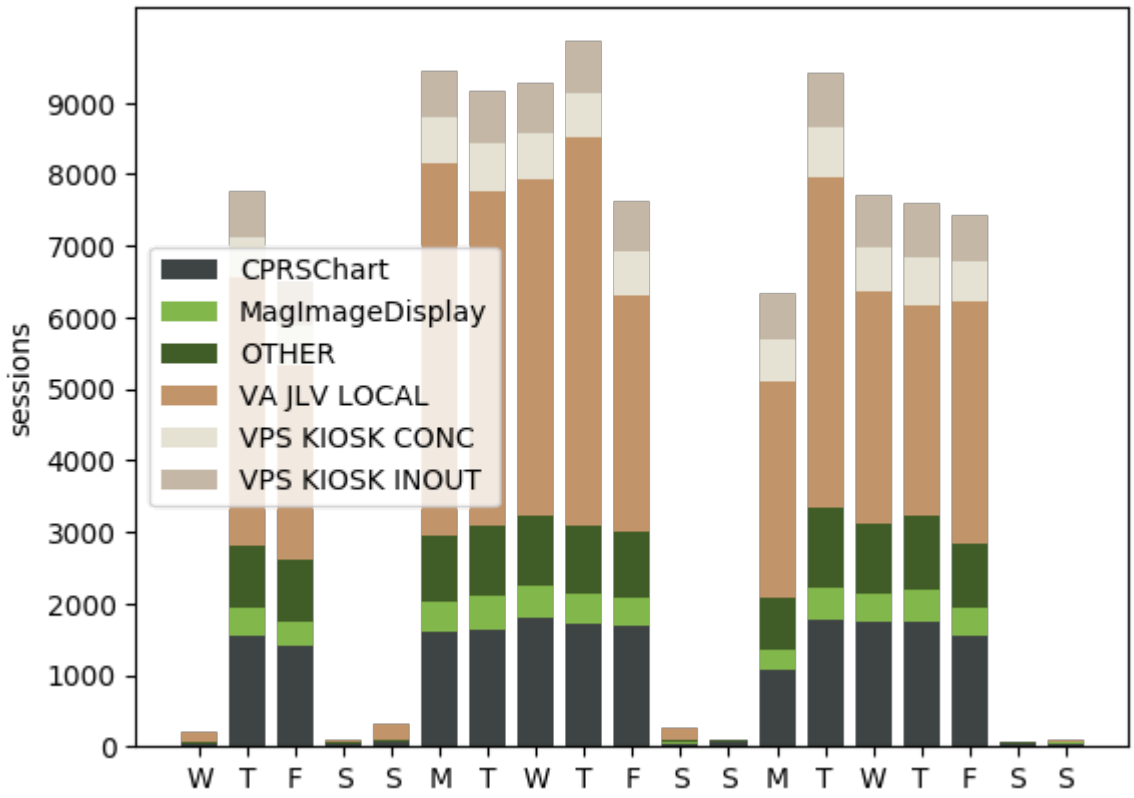
The following chart emphasizes *CPRS* has the highest number of users, followed by *VPS KIOSK*, Imaging Display (*MagImageDisplay*) and Clinical Scheduling (*ClinSchd*) …



Ranking clients by their traffic shows *CPRS* is even more dominant but also brings *JLV* (user rank 7) and the *PCERecordManager* (user rank 36) to the fore …



Ranking by session count promotes *JLV* further (rank 1) and pushes *CPRS* to second place …



JLV employed many sessions of short duration in parallel to bulk load a patient's record as quickly as possible. With *CPRS*, a user has only one long running session with traffic proportional to a user's screen activity. Both the nature of its traffic (bulk load of a patient record) and its approach to loading (parallel sessions) means that both the traffic rank (2) and session rank for JLV (1) was higher than its user rank would suggest (7).

Mirrored traffic contains identifiers of signed on users including VistA IEN, name, title (**99.64%** have titles), network identifier and for JLV, social security number. The following lists the top five user titles when user activity is ordered by traffic generated …

#	Title
1	**REGISTERED NURSE**
2	**MEDICAL SUPPORT ASSISTANT**
3	**PHYSICIAN**
4	**LVN**
5	**CLINICAL PHARMACY SPECIALIST**

Mirrored traffic also contains the IP address of clients. There are three flavors of IP - those from specific VA VistA stations ("*Station IPs*") such as *VCB* itself, those from *Citrix* ("*Citrix IPs*) and those from pools of IPs allocated to specific applications ("*Application Pool IPs*").

Only *Station IPs* identify where a client is connecting from. The monitored period shows that the vast majority of use of CPRS and other local end user clients was from VCB but there were sessions that originated elsewhere as well. This means that users at these other locations had PIV or Access Verify accounts in VCB VistA.

#	IP Group	Station	Example
1	**10.141**	**VCB [740]**	10.141.17.37
2	10.112		10.112.126.19
3	10.137	Waco [674]	10.137.176.45
4	10.138	Dallas [549]	10.138.161.181
5	10.140	San Antonio [671]	10.140.146.76
6	10.142	*VISN 17* (Texas)	10.142.9.8
7	10.154	Fort Harrison, MT (436)	10.154.248.112

4. Remote Signon Sessions

Remote Signons covers

> activity by end users from beyond VCB who logon using either the *CAPRI* or *BSE* sign on methods and activity by automated applications leveraging a small number of machine user accounts in the system.

Though these users accounted for far less traffic than their *Local* counterparts (**5.56 GB (10.9%)**) during the monitored period, there were more of them on an average weekday (**991** vs **790**) and they account for more of the system's sessions (**132,435 (57.16%)**).

There are three flavors of remote user, those using [1] JLV, those using a [2] client that employs BSE-login such as the VBA's **CAPRI GUI** and [3] remote machine users.

Remote JLV

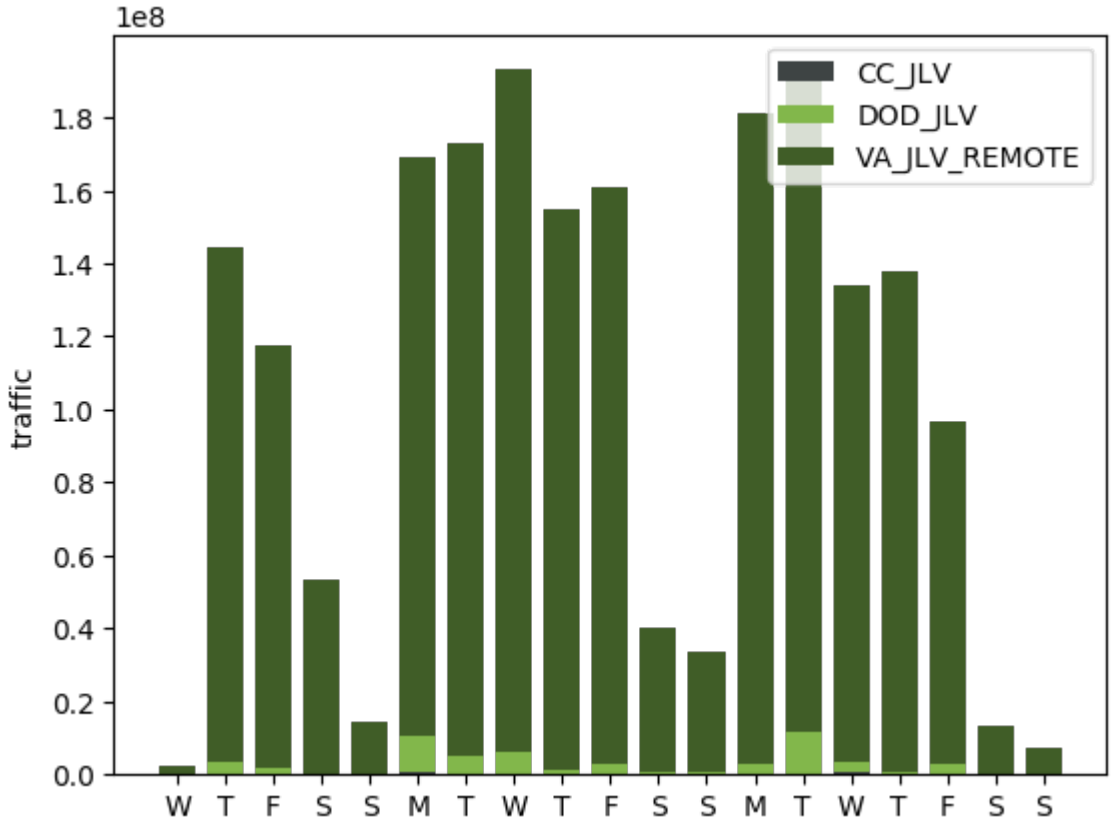
The use of JLV by local (VCB) users is included in the local signon session section above. JLV is primarily used by remote users to access the patient records of a VistA system. Remote use of JLV represented **3.96%** of traffic and **46.53%** of sign on sessions during the monitored period. As stated already above, JLV opens many sessions - a median of **12** - for each user login. This makes traffic numbers a better reflection of its activity ….

#	Name	Users (per day)	Traffic	Sessions	RPCs
1	**VA JLV REMOTE**	443/48	1.83 GB (97.31%)	104,141 (96.59%) - 8,454/939	1,061,931 (96.9%)
2	**DoD JLV**	15/0	49.21 MB (2.56%)	3,439 (3.19%) - 268/10	32,004 (2.92%)
3	**Community Care (CC) JLV**		2.59 MB		1,924 (0.18%)

Note that

- Most use was by VA users in remote locations. Each of these users would have a user record in VCB VistA by virtue of JLV's CAPRI based logins.
- JLV signs all DoD Users in as the same *"Department of Defense, User"*. A user with a similar name and the same synthesized social security number exists in every production VistA. The individual DoD identifier for end users is passed in by JLV and is available in the mirrored traffic.
- JLV signs all Community Care Users in as the same machine user. That user also has a synthesized social security number and appears in every production VistA. JLV appears to assign its own identifier to community care end users and that identifier is available in mirrored traffic. As so few of these users signed in during the monitored period, the median number of sign ins per day is 0. Were the number to increase, traffic monitoring could be used to tell a facility what community care doctors have logged on and what information they accessed including the specific patient records queried.

The following graphic highlights the dominance of VA users and the insignificance of community care use during the monitored period …



JLV sessions come from its own pool of IPs in the *10.206*, *10.224*, *10.227* ranges. During the monitored period, VA users logged in from **105** remote stations. These are the top five …

#	Remote Station
1	**DALLAS [549]**
2	**SAN ANTONIO [671]**
3	**HOUSTON [580]**
4	**WACO [674]**
5	**200CORP**

where 200CORP appears to signify VBA use. Top access was from adjacent Texas locations but lessor access occurred from all over the VA from New York to Hawaii.

Remote BSE

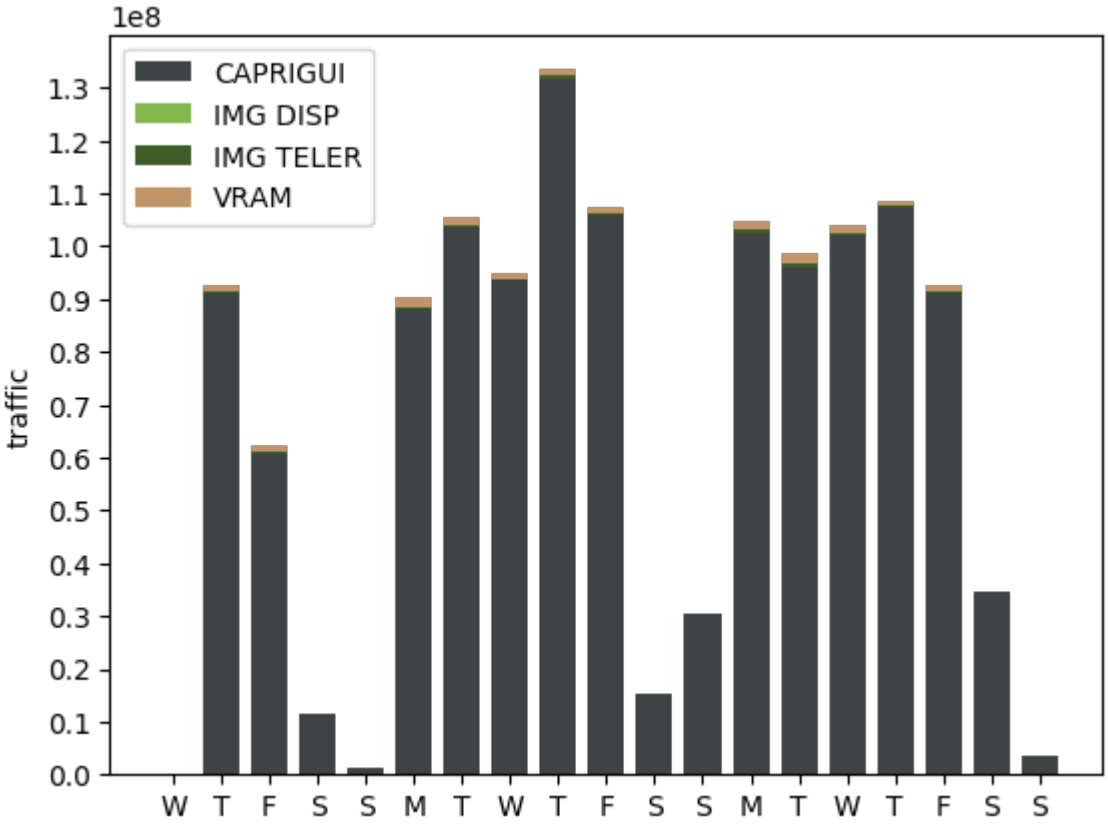
4 types of client used BSE to login to *VCB* VistA, *CAPRI GUI* (used by VBA), *VRAM* (used by Voucher Examiners) and two flavors of VistA Imaging, Display and TeleReader. Collectively they account for **2.36%** of traffic and **9.11%** of sessions seen during the monitored period.

#	Name	Users (per day)	Traffic	Sessions	RPCs
1	**CAPRI GUI**	384/26	1.18 GB (98.29%)	18,532 (87.81%) - 1,449/102	1,258,062 (90.55%)
2	VRAM	143/5	15.97 MB (1.3%)	2,453 (11.62%) - 174/8	103,327 (7.44%)
3	VistA Imaging TeleReader	5/0	4.94 MB	103 (0.49%) - 8/0	27,520 (1.98%)
4	VistA Imaging Display		205.49 KB		459 (0.03%)

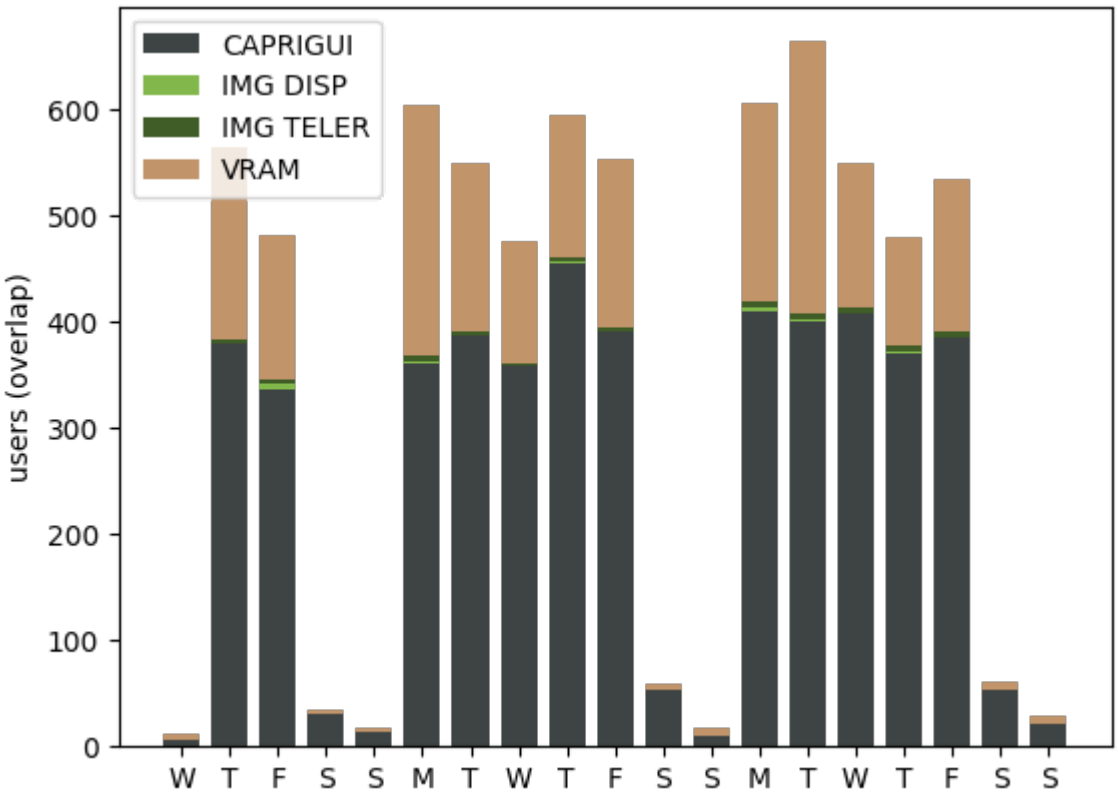
Note that:

- VBA-used *CAPRI GUI* dominated traffic and users. Despite having the same name as “CAPRI”, the sign on method, this client logs in with the stronger BSE method. Note that use doesn’t stop on the weekend. This client uses a lot of direct database access RPCs. This makes it difficult but not impossible to know exactly what it is doing. Such broad access to any system is not desirable, particularly a system with as much PII/PHI as VistA.
- VistA Imaging Display was so rarely used that daily median user number is 0. It came from a series of locations including Connecticut, Pennsylvania and Wyoming
- VRAM had proportionally more sessions and many more users than its traffic suggests. Note that it was also used by some local users and that use is accounted for in the Local Signon section above
- VistA Imaging TeleReader access was all by a series of users from Waco, Texas (674)
- Both VRAM and CAPRI GUI are validated against one central VistA and not VistAs distributed across the VA. This means the BSE sign on itself doesn’t identify a user’s remote location. However, CAPRI GUI comes from a range of IPs that could be mapped and were traffic mirroring added to BSE VistA callback connections, extra information about user locations would be fully available.

The following graphs highlight CAPRI GUI’s dominance of traffic …



and VRAM's proportionately higher number of users …



Remote Machine

4 *Machine* user accounts were employed by automated clients to login to VistA. These clients accounted for **4.85%** of traffic and **1.52%** of sessions during the monitored period.

Client	Machine User	Access Method	Traffic	Sessions (Week/End)
"DOD VHAPALAPPMDO"	DoD User	CAPRI (LOA 1)	2.3 GB (92.77%)	18/13
VPS KIOSK	CONNECT,VPS	Access Verify	102.16 MB (4.03%)	18/15
FBCSAuthorization	User, Fee Clerk	Access Verify	75 MB (2.96%)	142/138
FBCSAuthorization	User, Fee Supervisor	Access Verify	5.98 MB	8/2

Note that:

- *"DOD VHAPALAPPMDO"* is named for the user it logs into in VCB VistA and for part of the hostname of its IP addresses. Though it employed few sessions, it dominated traffic. It logs in using CAPRI to the same machine user employed by *JLV DoD*. It accesses before business hours, comes from overlapping sessions from five IPs of form *VHAPALAPPMDO{XXX}.v21.med.va.gov* and employs "direct to database" RPCs to bulk download records. It appears to be a batch data cacher, a task better performed in VAEC by a scheduled background job that avoids the RPC Interface.
- Only *VPS KIOSK (CONNECT,VPS)* came from a local IP address, *10.141.160.197*. It may be more appropriate to count it among local users in a new Local Machine User category.
- Both *FBCSAuthorization* clients came from the Austin Automation Center, specifically from *vaausappfbc309.aac.dva*.

5. Recommendations

1. Turn off “Health Check” Sessions, the 50%+ of sessions that fail to sign in and appear to check if it is still operating. VistA’s health should be monitored with standard VAEC-mechanisms if it isn’t already.

2. Retire CAPRI (LOA 1): this is a check-free “honor system” which leaves VistA in a completely open condition.
    - The Automated Client, *“DOD VHAPALAPPMD”* which logs into VistA using CAPRI (LOA 1) and bulk loads data with direct access to VistA’s database interface should be replaced by a VAEC-based scheduled task. Such bulk downloads shouldn’t be performed over the RPC interface.
    - JLV should move to BSE-based logins if VistA’s current support for PIV doesn’t support JLV’s requirements

3. The much-used VBA CAPRI GUI employs a series of “direct to database” RPCs instead of easier to monitor, task-specific calls. Such direct database access is almost never permitted to mainstream clients today, particularly to those accessing a server with as much PII/PHI as VistA. Either this client needs to be rewritten and replaced or the nature of its calls need to carefully examined and their exact use enforced. This would prevent neferious clients from masking as CAPRI GUI and using similar direct database access to pull any data from a VistA without limit.

4. Some local users sometimes use a client with PIV but at other times use Access Verify with the same client. This use should be investigated. Preferably, where a client supports PIV, users should employ one at all times.

5. If VA’s policy is that users can only login with PIV or Access Verify to their home VistA then remote users should not have PIV or Access Verify enabled accounts in VCB VistA.

6. Machine “users” - proxy accounts used by clients - present obvious points of vulnerability. If VistA is to continue to support such accounts, access should only be permitted from strictly managed access services such as JLV’s JMDWS and its known IP pool. Preferably access services such as this should be housed in VAEC and broad VA network access should not be allowed to these “users”.

7. A real-time interface monitor should log all RPC sessions to VistA, identifying users, clients, any patient selections made and note unusual behavior for sessions of their kind.

8. The need to upgrade VistA to improve user authentication has hampered the VA’s efforts in this area for many years. VistA user authentication should move out of VistA and be centralized in a VAEC-based authentication service.
    - Through the use of “RPC Emulation”, a PIV-supporting service could allow incremental upgrades to “VistA Security” without requiring changes to VistA or its clients
    - BSE validation could execute against such a service instead of individual “Home VistAs”. For VAEC-resident VistA’s, this would avoid connections across the TIC to VistAs still housed in VA data centers.