ClearPass Operational Report Detail

Derin Mellor

18/12/20

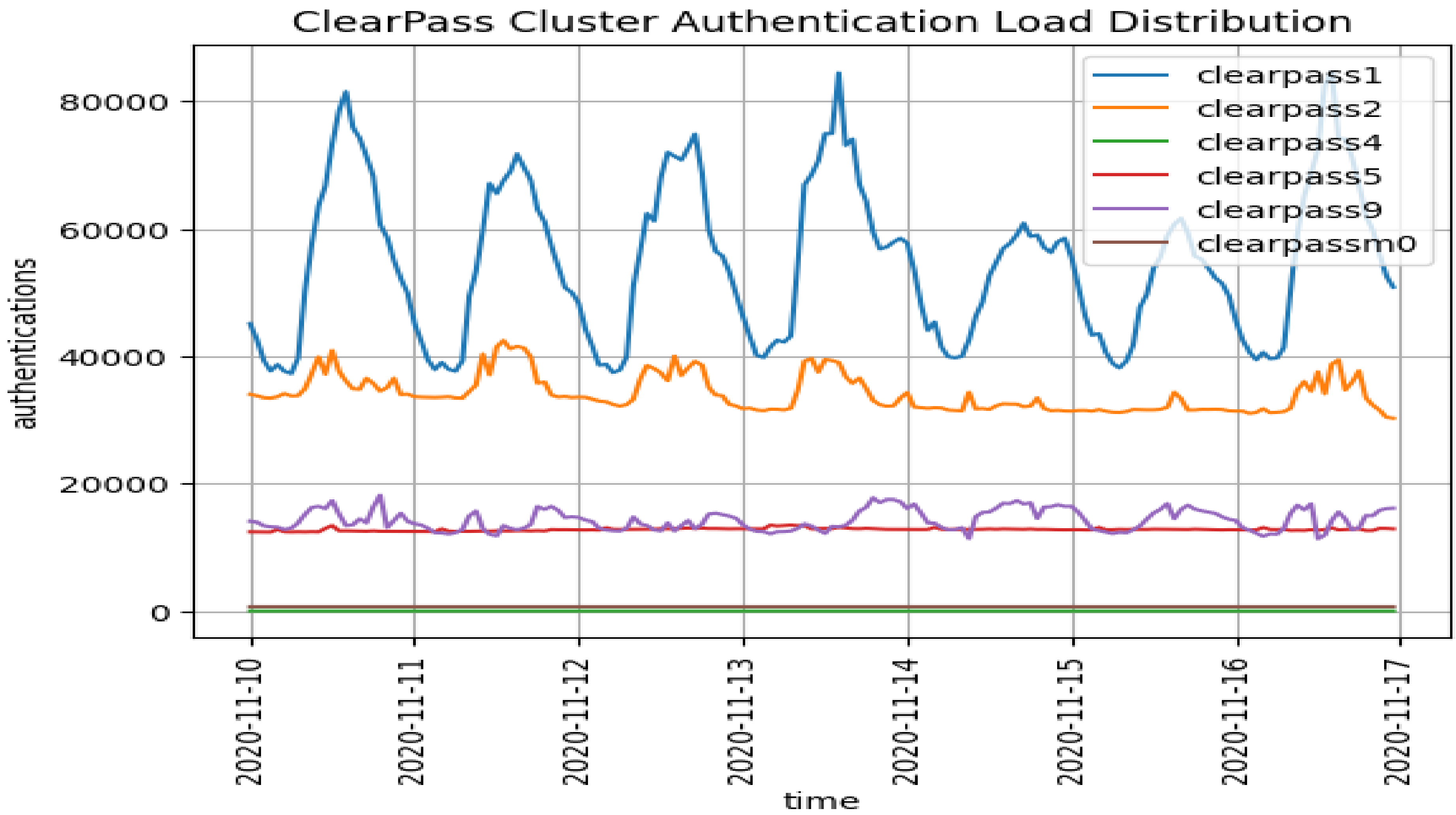
0.03 DRAFT

Time Frame 2020-11-10 to 2020-11-17

Contents

Specific Details

ClearPass Cluster Authentication Load Distribution



This graph may highlight poor distribution of authentications across the ClearPass cluster. However, this is very dependent on the cluster's architectural design.

If this is a master/hot-standby design you expect the load to be totally on the master and only transition to the hot-standby if the master has failed.

If this was a distributed design one would expect the load to be evenly shared across all the ClearPass appliances. A quick visual inspection will indicate how well this is operating.

ClearPass Cluster Details

This reports all the ClearPass appliances that had been involved in RADIUS authentications

ClearPass	IP	Zone
clearpass1	144.32.128.78	default
clearpass2	144.32.128.122	default
clearpass4	144.32.129.238	default
clearpass5	144.32.11.2	default
clearpass9	144.32.128.156	default
clearpassm0 (Publisher)	144.32.128.68	default

Top 10 ClearPass Cluster Events

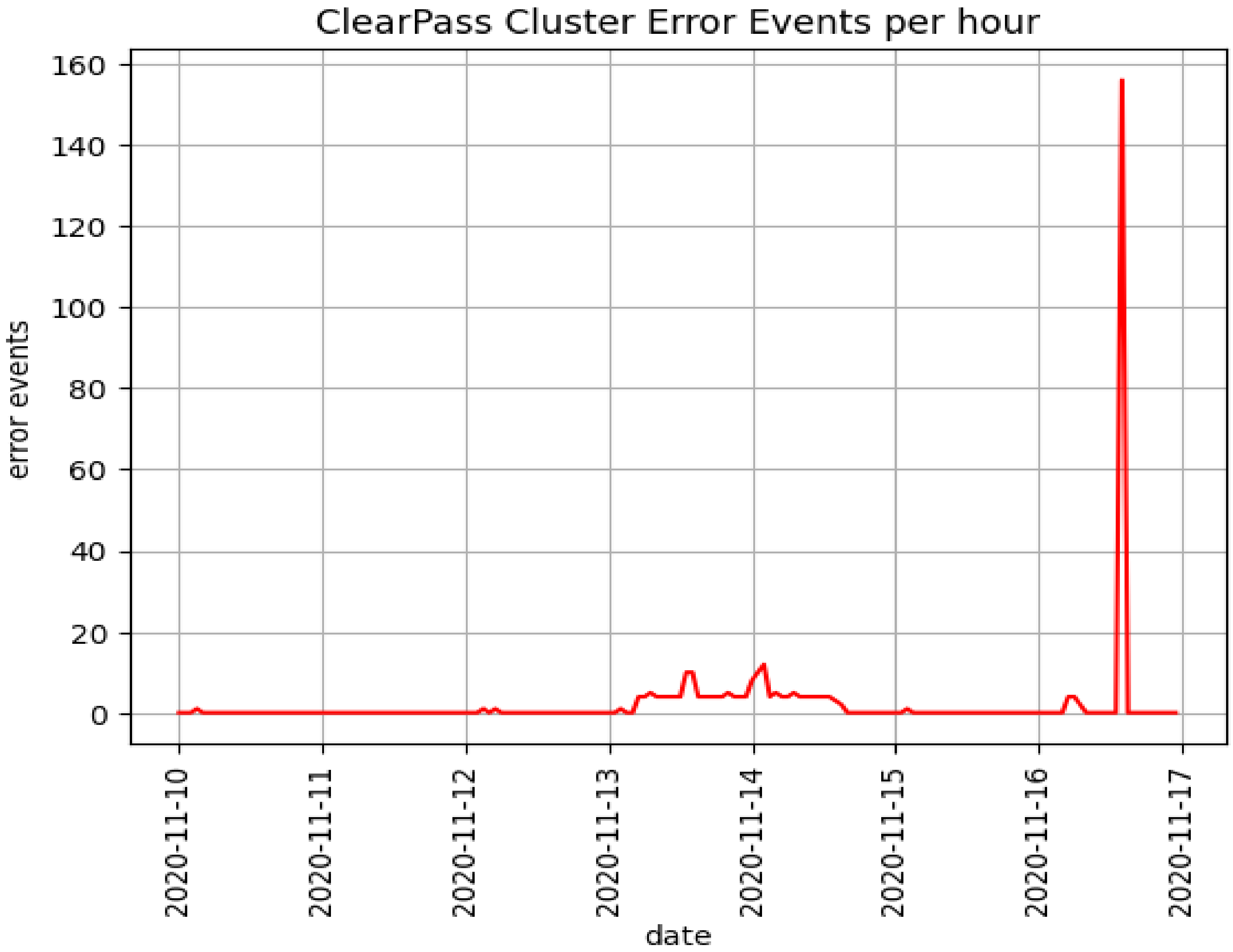
NOTE: ERROR in Red & WARNING in Amber

Count	ClearPass	Source	Level	Category	Description
169	clearpass1	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=10.4.100.169
168	clearpass2	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=10.4.100.19
168	clearpass9	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device 10.4.100.179 with error=Authorization error\nReading sysObjectId failed for device=10.4.100.179\nReading switch initialization info failed for

					10.4.100.179
166	clearpass4	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device 10.4.100.203 with error=No response received\nReading sysObjectId failed for device=10.4.100.203\nReading switch initialization info failed for 10.4.100.203
165	clearpass9	SnmpService	WARN	ReadDeviceInfo	Error fetching table qbridgeFdb. Agent did not return variable bindings in lexicographic order.\nError fetching table qbridgeFdb. Agent did not return variable bindings in lexicographic order.\nFailed to read port to MAC address table from NAD=10.4.100.27\nReading MAC addresses behind ports failed for switch=10.4.100.27\nReading switch information failed for 10.4.100.27
165	clearpass1	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device 10.4.204.170 with error=No response received\nReading sysObjectId failed for device=10.4.204.170\nReading switch initialization info failed for 10.4.204.170
163	clearpass4	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=10.4.100.4
162	clearpass2	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device 10.4.100.205 with error=No response received\nReading sysObjectId failed for device=10.4.100.205\nReading switch initialization info failed for 10.4.100.205
161	clearpass4	SnmpService	WARN	ReadDeviceInfo	SNMP GET failed for device 10.4.75.82 with error=No response received\nReading sysObjectId failed for device=10.4.75.82\nReading switch initialization info failed for 10.4.75.82
160	clearpass2	SnmpService	WARN	ReadDeviceInfo	Failed to discover engineId\nReading SNMP v3 engineId failed for device=10.4.100.43

This reports the number of matching events and which ClearPass they occurred on. Error events are highlighted in red. Warning events are highlighted in red. Ultimately it is desirable to minimise these.

ClearPass Cluster Error Events per hour



This graph summaries the ClearPass cluster's error events. Clearly any error events are not good, but may not be directly related to authentications. If these do correlate with increased authentication failures they should be investigate.

ClearPass Cluster Error Events Burst Details

These tables highlights the break down of events in key bursts

Event burst between 2020-11-16 14:00-2020-11-16 15:00

Count	ClearPass	Category	Description
150	clearpass1	Authentication	RADIUS authentication attempt from unknown NAD 10.4.59.14:4012
6	clearpass5	Authentication	RADIUS authentication attempt from unknown NAD 10.4.59.14:4012

Top 10 ClearPass Cluster Alerts

NOTE: Red threshold=2100, Amber threshold=210

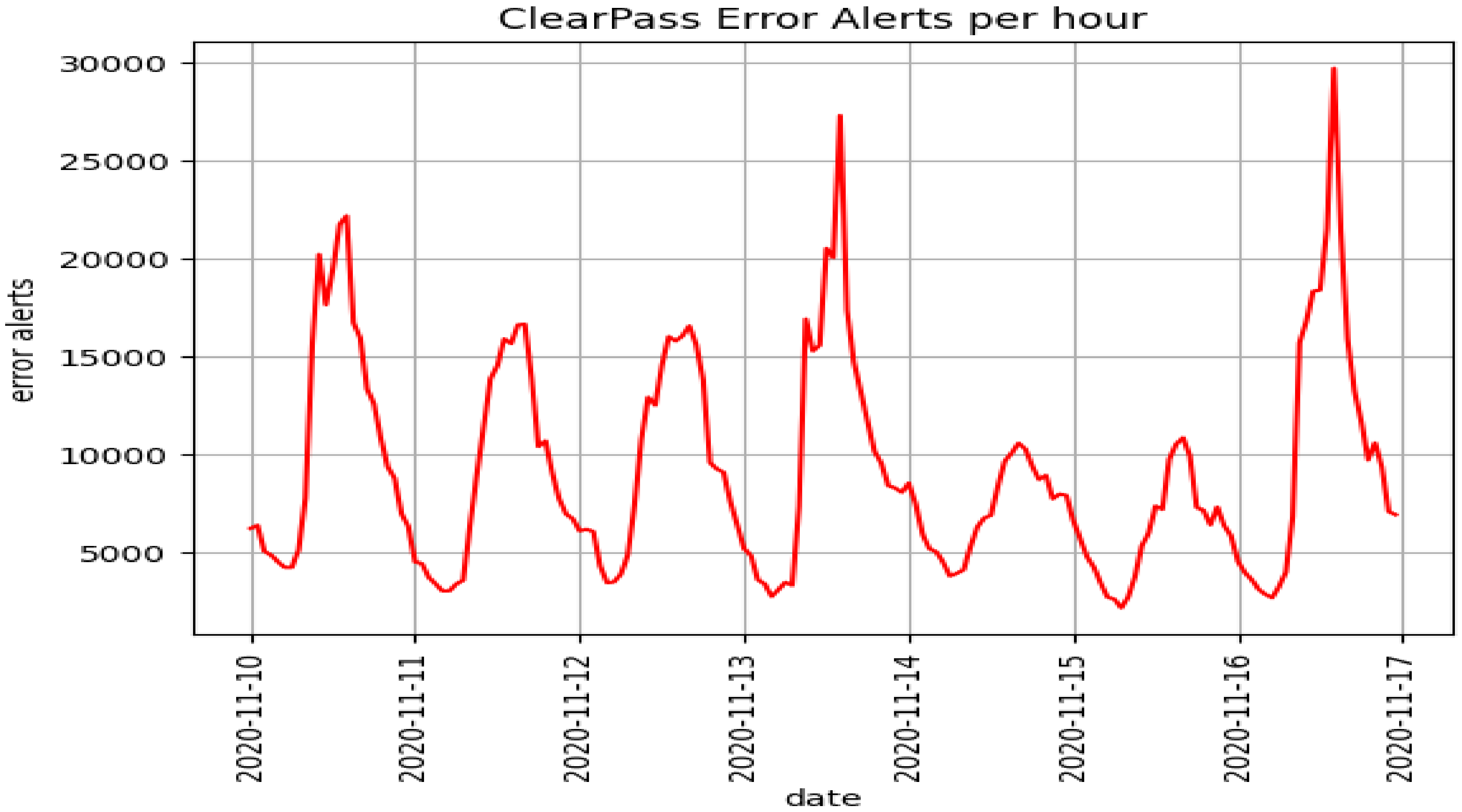
Totals	Service Name	Alert
529082	RADIUS	Client did not complete EAP transaction
444766	RADIUS	[Guest Device Repository] - localhost: User not found.\nMAC-AUTH: MAC Authentication attempted by unknown client, rejected.
218346	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nCannot select appropriate authentication method
117166	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: warning alert by client - close_notify\nTLS Handshake failed in SSL_read with error:140940E5:SSL routines:ssl3_read_bytes:ssl handshake failure\neap-tls: Error in establishing TLS session
66643	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User

		not found.\n[Local User Repository] - localhost: User not found.\nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure
54079	RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) \nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure
33611	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: fatal alert by client - unknown_ca\nTLS Handshake failed in SSL_read with error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca\neap-tls: Error in establishing TLS session
10926	RADIUS	Request rejected by home server eduroam4.york.ac.uk
10700	RADIUS	Request rejected by home server eduroam2.york.ac.uk
10606	RADIUS	Request rejected by home server eduroam3.york.ac.uk

NOTE:Alert Whitelist 'Failed to get value for attributes=%'

Alerts are raised by Insight. Custom alerts can be created in Insight. This reports the number of matching error events that occurred. Thresholds, defined in the Error events are highlighted in red. Warning events are highlighted in red. Ultimately it is desirable to minimise these.

ClearPass Error Alerts per hour



NOTE: Alert Whitelist 'Failed to get value for attributes=%'

This graph summaries the ClearPass cluster's error Alerts. Clearly these are not good, but may not be directly related to authentications. If these do correlate with increased authentication failures they should be investigate.

ClearPass Error Alerts Details

This table shows the the common alerts above the threshold

NOTE: Threshold=300

Event burst between 2020-11-16 14:00-2020-11-16 15:00

Count	Service	Alert
12836	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nCannot select appropriate authentication method
7719	RADIUS	Client did not complete EAP transaction
3792	RADIUS	[Guest Device Repository] - localhost: User not found.\nMAC-AUTH: MAC Authentication attempted by unknown client, rejected.
2236	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: warning alert by client - close_notify\nTLS Handshake failed in SSL_read with error:140940E5:SSL routines:ssl3_read_bytes:ssl handshake failure\neap-tls: Error in establishing TLS session
757	RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) \nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure
588	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: fatal alert by client - unknown_ca\nTLS Handshake failed in SSL_read with error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca\neap-tls: Error in establishing TLS session
423	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD

		machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\n[Local User Repository] - localhost: User not found.\nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure

Event burst between 2020-11-13 14:00-2020-11-13 15:00

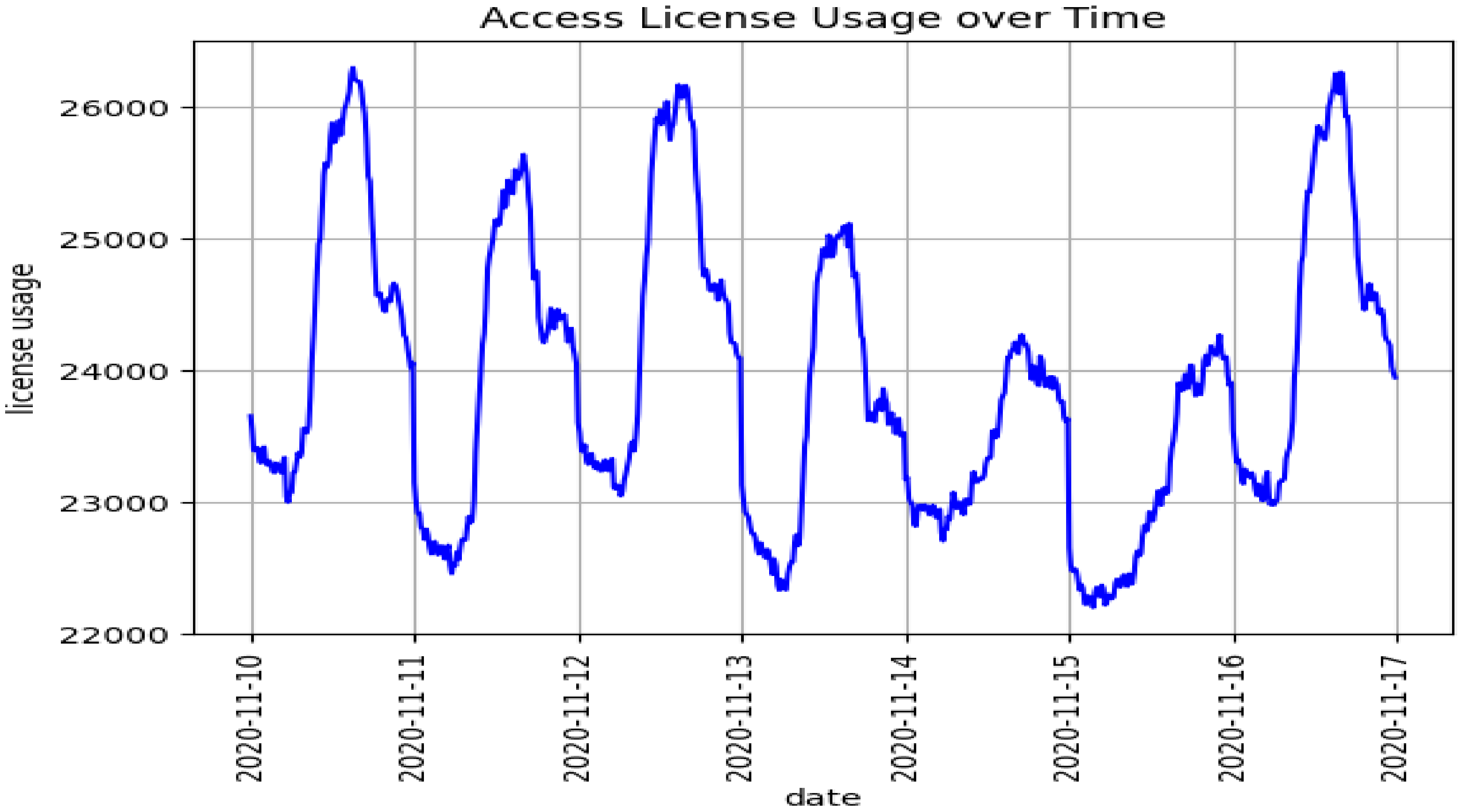
Count	Service	Alert
9777	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nCannot select appropriate authentication method
8309	RADIUS	Client did not complete EAP transaction
3707	RADIUS	[Guest Device Repository] - localhost: User not found.\nMAC-AUTH: MAC Authentication attempted by unknown client, rejected.
2870	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: warning alert by client - close_notify\nTLS Handshake failed in SSL_read with error:140940E5:SSL routines:ssl3_read_bytes:ssl handshake failure\neap-tls: Error in establishing TLS session
791	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: fatal alert by client - unknown_ca\nTLS Handshake failed in SSL_read with error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca\neap-tls: Error in establishing TLS session
783	RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) \nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure

Event burst between 2020-11-10 14:00-2020-11-10 15:00

Count	Service	Alert
8437	RADIUS	Client did not complete EAP transaction
4023	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: warning alert by client - close_notify\nTLS Handshake failed in SSL_read with error:140940E5:SSL routines:ssl3_read_bytes:ssl handshake failure\neap-tls: Error in establishing TLS session
3706	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nCannot select appropriate authentication method
3022	RADIUS	[Guest Device Repository] - localhost: User not found.\nMAC-AUTH: MAC Authentication attempted by unknown client, rejected.
961	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: fatal alert by client - unknown_ca\nTLS Handshake failed in SSL_read with error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca\neap-tls: Error in establishing TLS session
601	RADIUS	MSCHAP: AD status:Logon failure (0xc000006d) \nMSCHAP: Authentication failed\nEAP-MSCHAPv2: User authentication failure
391	RADIUS	UoY AD Authentication - itsdc0.its.york.ac.uk: User not found.\nUoY AD Auth service accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Machine Identification - itsdc0.its.york.ac.uk: User not found.\nUoY AD machine accounts - itsdc0.its.york.ac.uk: User not found.\nUoY Computer Object Identification - itsdc0.its.york.ac.uk: User not found.\nHYMS AD - 240820 - hymsdc2.hyms.ac.uk: User not found.\nEAP-PEAP: fatal alert by client - access_denied\nTLS session reuse error

NOTE:Alert Whitelist 'Failed to get value for attributes=%'

Access License Usage over Time



These highlights when licenses are being used. If the report is over a long period of time it may indicate changes in network usage. Unexpected peaks may indicate malicious behaviour.

Stale Access License Recover

Nothing exceptional

These are a count of 'stale' access licenses that are recovered overnight. An access license becomes 'stale' if after 24 hours ClearPass has not seen a RADIUS Accounting Interim or a RADIUS Accounting Stop. The session may still exist but ClearPass has no visibility or control over it.

Endpoint Categorization

Category	Total
SmartDevice	9957
No Fingerprint	3733
Home Audio/Video Equipment	87
Computer	5329
Network Boot Agents	38
Projectors	1
Audio/Video Devices	3
Monitoring Devices	18
Building Automation	3
Point of Sale devices	3

This reports the top 10 endpoints of particular type.

Endpoints reported as 'No Fingerprint' are highlighted in red: These have not been fingerprinted - question is why? This could indicate lack of DHCP Request or no proactive scanning?

Endpoints reported as 'Generic' are highlighted in amber: These either have been fingerprinted purely on the OUI or the fingerprint is not recognised. If only an OUI why? If the fingerprint is not recognised best to feed this information back via Aruba TAC - they will update the fingerprint file appropriately (this is automatically loaded on the 1st or 15th of every month) Alternatively, manually create the appropriate fingerprint categorization.

Endpoint IP Address Assignment

Total	Static IP	DHCP Address
27076	4075	23001

This reports the distribution between devices with static IP address and using DHCP. ClearPass assumes all devices have a static IP address and only makes the device 'DHCP' if it receives an associated DHCP Request relayed to ClearPass (usually). Generally, it is preferred to use dynamic IP addresses. Hence, if the Static IP count is greater than the DHCP count it is reported in amber. This could be an indication that there are excessive number of devices with a static IP address. Or that DHCP Requests are not being relayed to the ClearPass.
DHCP is highly desirable that ClearPass receives DHCP Requests as it can use these to profile the device, and possibly identify spoofed devices.
Static IP addresses can be profile using SNMP, SSH, WMI, NMAP or device's HTTP user-agent (reliant on ClearPass seeing the web request). NMAP and user-agent are both very unreliable for fingerprint, but may be useful to identify specific usage or spoofing.

Endpoint MAC & IP Address Details

Total	MAC Only	MAC & IP	IP Only
27076	3280	23785	11

This reports the number of devices that ClearPass knows - this is split in to three categories:
1) Devices with MAC address only: Possibly indicates that RADIUS Account is not working or the RADIUS Accounting is not populating the Framed-IP-Address. If the NAS does not support RADIUS Accounting with Framed-IP-Address ClearPass can be configured to read the appropriate ARP table (e.g. local access router) - using the suitable SNMP credentials. NOTE the default poll is once an hour, this can be tuned down to 10 minutes. But this is likely to be too slow for effective RESTful API upper-layer injection where the IP address is required (e.g. firewall). These are always highlighted in amber. Also NASs dealing with devices that have static IP addresses are likely to require special configuration to proactively set the Framed-IP-Address - some NAS do not support this or are slow at learning a static IP addresses.
2) Devices with MAC and IP address: This is where we want everything.

3) Devices with IP address only: These are devices that typically have been learnt via a proactive scan (SNMP, SSH, WMI or NMAP) or via ClearPass observing the device's HTTP user-agent. These could be devices that are not being controlled by ClearPass? - these need checking.

Endpoints with Randomized MAC Addresses

Total	0

This is the total number of endpoints using randomized MAC addresses. Theoretically you should only see this on devices connecting to open SSID.

Number of Suspected Spoofs Detected

3669

Device spoofing is a serious concern. Though ClearPass' ability to detect them is not great. False positives are common. Likewise, many devices my be commissioned using PXE Boot - there is a setting to disable identifying these. Alternatively whitelist in this report's ini file.

10 Most Recent Spoof

MAC	Category	Family	DevType	Spoof Category	Spoof Family	Spoof DevType
5882a8945439	Computer	Windows	Surface	Computer	Windows	Surface
5ae85857fded	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X
ccd9ac748137	Computer	Windows	Windows	Computer	Windows	Windows

e4aaeac5146d	Computer	Windows	Windows	Building Automation	Liteon	Liteon Storage
f01dbc21d29a	Game Console	Microsoft	Xbox	Computer	Windows	Windows 10
800c67c22516	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X
28cfe91d3ded	Computer	Apple Mac	Mac OS X	SmartDevice	Apple	Apple iOS Device
e4aaeae290d5	Computer	Windows	Windows	Building Automation	Liteon	Liteon Storage
640bd7baaa29	SmartDevice	Apple	Apple iPad	Computer	Apple Mac	Mac OS X
2659c22a6afe	SmartDevice	Apple	Apple iPhone	Computer	Apple Mac	Mac OS X

Missing Known Endpoints

52199

Last Seen	MAC Address	IP Address	Hostname	Username	NAS Name	NAS IP	Media	Port/SSID
2020/11/09	2cf0a2d0268d	10.240.22.25	francishellyeah	fs1038	arubal1-vip	144.32.64.35	Wifi	eduroam
2020/11/09	c8f733da28c0	10.240.250.120	joon	hk1030@york.ac.uk	arubamm	144.32.76.60	Virtual	
2020/11/09	e0b55f92e837	fe80::1cdf:beb7:5b4:d7	ipad	mk1463	arubamm	144.32.76.60	Wifi	eduroam
2020/11/09	b00594423b65	fe80::b205:94ff:fe42:3b			arubal3-vip	144.32.64.39	Wifi	mydevices
2020/11/09	2e1286686dab				arubal3-vip	144.32.64.39	Wifi	mydevices
2020/11/09	8864408aab8e				arubal3-vip	144.32.64.39	Wifi	eduroam
2020/11/09	ccd281e7b186	fe80::46a:b063:e777:a		xs924@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam
2020/11/09	caab01291e89	10.240.203.219	mas-iphone	mdor500	arubal2-vip	144.32.64.37	Wifi	eduroam
2020/11/09	b88687961e2c	10.240.116.147	opeyemi-pc	ta878@york.ac.uk	arubamm	144.32.76.60	Wifi	eduroam
2020/11/09	f0a35a71f977	fe80::1c51:7bc2:fc9:3b	arya		arubal3-vip	144.32.64.39	Wifi	mydevices

This indicates the number of Known endpoints that have not connected in the time frame of the report. WARNING: This maybe misleading as the Insight database does not indicate whether a Known endpoint has been deleted.

Authentications per Service

Service	Total	Successes	Failures
UoY Generic MacAuth - 280620	6488175	6488175	0
UoY Health-Check - 280319	6161234	6160655	579
UoY Eduroam Authentication - 041219	5036586	4269361	767225
UoY Aruba Generic MacAuth - 201020	598645	598645	0
UoY PSK Net 140220	564094	119273	444821
UoY What the hell are these devices - 051219	192087	0	192087
Eduroam Visitor Wireless - 211119	178028	103364	74664
UoY IoT MacAuth - 161020	87931	87931	0
UoY AirGroup Authorization Service - 140319	72618	72618	0
UoY WebVpn Service - 030719	35502	33414	2088
UoY Airwave logon 030317	30287	29	30258
UoY 802.1x ArubaOS Wired - 051219	28500	28080	420
UoY Block invalid eduroam access - 050615	27995	0	27995
UoY Aruba Controller Authentication - 140217	20085	20084	1
UoY eapol_test TLS service - 120419	19614	19614	0
New Eduroam Visitor Healthcheck - 070316	19589	19569	20
UoY Comware Switch Authentication - 121120	14623	14620	3
UoY 802.1x Procurve Wired - 051219	13299	13221	78
UoY IoT TLS service - 170518	10719	3998	6721
UoY 802.1x Comware Wired - 310120	10259	8705	1554
UoY Comware Switch Authentication - 260117	7824	7822	2
UoY Managed Laptop Eduroam Authentication - 240820	7440	7078	362
UoY Procurve Switch Authentication - 121120	4394	4394	0
UoY Procurve Switch Authentication - 181018	3221	3221	0
UoY ArubaAP Wired Port 802.1X - 051219	2355	2331	24
UoY ArubaOS Switch Authentication - 121120	1912	1912	0

UoY ArubaAP Wired Port Macauth - 191020	1764	1098	666
UoY 802.1x Procurve 2650 Wired - 051219	1451	1428	23
UoY ArubaOS Switch Authentication - 090318	1373	1373	0
UoY Comware 5500 Switch Authentication - 121120	1281	1266	15
UoY IMC Auth - 051219	673	0	673
UoY machine auth - 130319	610	195	415
UoY Wireless Groupcycle MacAuth - 161020	501	501	0
UoY Comware 5500 Switch Authentication - 140217	455	455	0
UoY wireless machine auth - 161020	320	195	125
No Match	232	0	232
UoY Procurve 2650 Switch Authentication - 121220	153	153	0
UoY Guest Operator Logins - 171218	139	131	8
ITSYORK Eduroam Authentication - 080915	129	122	7
UoY Procurve 2650 Switch Authentication - 160517	114	114	0
[Device Registration Disconnect]	79	79	0
Fortinet FW Authentication - 02032016	12	9	3
UoY IMC logon 031117	9	7	2
UoY Insight Operator Logins - 220618	7	7	0
ITSYORK Wired Authentication - 030719	6	6	0
UoY Eduroam Visitor Wired - 030719	6	6	0

This orders the services based on the total number of authentications handled. It might be desirable to order the services so that the most commonly hit are near the top, though this is not likely to make much difference in performance.

Top 15 Failed Authentications per Server

NOTE: Red >= 50% & Amber >= 25%

Service	Total	Successes	Failures	% Failed
UoY What the hell are these devices - 051219	192087	0	192087	**100**
UoY Block invalid eduroam access - 050615	27995	0	27995	**100**
UoY IMC Auth - 051219	673	0	673	**100**
No Match	232	0	232	**100**
UoY Airwave logon 030317	30287	29	30258	**99**
UoY PSK Net 140220	564094	119273	444821	**78**
UoY machine auth - 130319	610	195	415	**68**
UoY IoT TLS service - 170518	10719	3998	6721	**62**
Eduroam Visitor Wireless - 211119	178028	103364	74664	**41**
UoY wireless machine auth - 161020	320	195	125	**39**
UoY ArubaAP Wired Port Macauth - 191020	1764	1098	666	**37**
Fortinet FW Authentication - 02032016	12	9	3	**25**
UoY IMC logon 031117	9	7	2	**22**
UoY Eduroam Authentication - 041219	5036586	4269361	767225	**15**
UoY 802.1x Comware Wired - 310120	10259	8705	1554	**15**

This is based on the percentage failure. Anything about 50% failure rate is highlighted in red. Above 25% is highlighted in amber. These should be investigated to understand why such high failure rates. It is highly desirable to minimize failures.

Top Endpoints not Matching a Service

NOTE: Red threshold=2100 , Amber threshold=210

#	MAC	Username	NAS	NAS IP	Media	Port/SSID
3	40b93cdfe8ba	service_radiushcheck	lfa4st1	10.4.61.92	Wired	
3	2c233af6433b	service_radiushcheck	l3st1	10.4.59.79	Wired	
3	ec9b8b23a5d0	service_radiushcheck	lmb1st1	10.4.214.102	Wired	
3	40b93ce061da	service_radiushcheck	lfa3st1	10.4.61.89	Wired	
3	40b93ce0671a	service_radiushcheck	lfa3st2	10.4.61.90	Wired	
3	e8f7244dbf85	service_radiushcheck	Cse4st3	10.4.48.93	Wired	
2	40b93ce43e52	service_radiushcheck	lfa2st1	10.4.61.94	Wired	
2	40b93c782d78	service_radiushcheck	xc1st1	10.4.60.9	Wired	
2	78929cd1e6d8	info-display-5F69@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam
2	2ad16b45b636	yw2683@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam
2	26f699b08ed7	pg877@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam
2	2c233a3e993d	service_radiushcheck	g1st1	10.4.75.49	Wired	
2	1ac8276195dd	@york.ac.uk	arubal1-vip	144.32.64.35	Wifi	eduroam
2	1ac2f7808462	@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam
2	2241ed1e090c	@york.ac.uk	arubal3-vip	144.32.64.39	Wifi	eduroam

Authentication request that don't match a service will be rejected. But why did that request not match a service? These needs investigating...

Top Wired Endpoints Authentications

NOTE: Red threshold=1750 , Amber threshold=175

Auths	Success	Failed	MAC
38706	38706	0	001a1e04e198
37539	37539	0	74d4351aa284
29744	29744	0	001a1e04e2b8
26208	26207	1	943fc2f02e3d
26208	26207	1	5c8a384b07c7
24978	24978	0	0090aa0567e8
24978	24978	0	0090aa0566dd
24976	24976	0	0090aa0143c3
24642	24642	0	0090aa0567f4
24194	24192	2	40b93c8aded7
24193	24190	3	e8f724485072
24192	24192	0	e8f7244ae3c3
24192	24192	0	40b93c780378
24192	24192	0	ec9b8b23a750
24192	24192	0	ec9b8b23a690

These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

MAC '001a1e04e198' Authentication Details

Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
9915	Success		UoY Generic MacAuth - 280	lmb1st3	10.4.214.104	slot=9;subslot=0;port=48;vlanid=4061

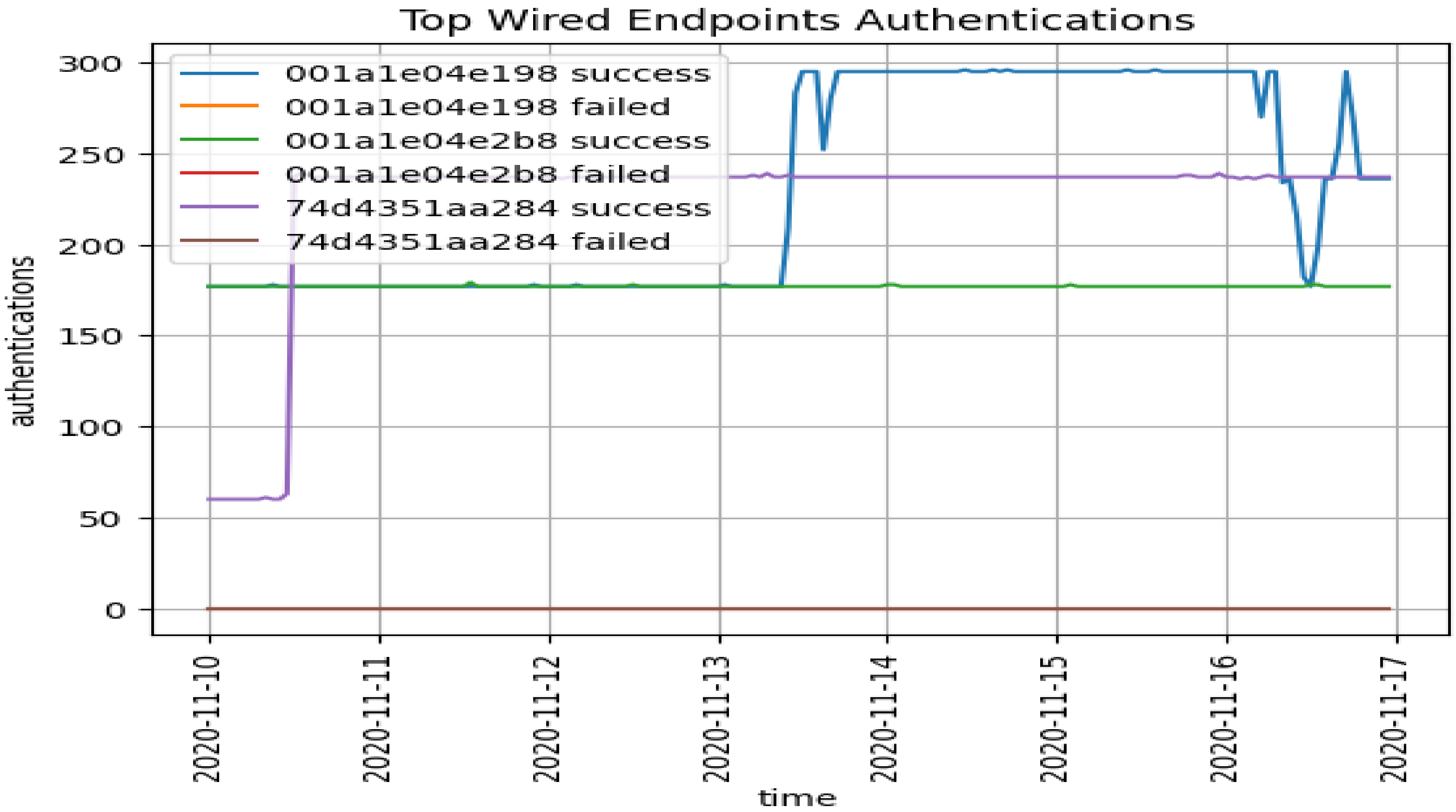
9914	Success		UoY Generic MacAuth - 280	Cse2st3	10.4.48.87	slot=4;subslot=0;port=47;vlanid=3737
9914	Success		UoY Generic MacAuth - 280	slb1st2	10.4.228.3	slot=9;subslot=0;port=45;vlanid=3721
4250	Success		UoY Generic MacAuth - 280	lmb2st2	10.4.214.137	slot=9;subslot=0;port=6;vlanid=4061
3984	Success		UoY Generic MacAuth - 280	lmb3st1	10.4.214.139	slot=3;subslot=0;port=16;vlanid=4061
432	Success		UoY Generic MacAuth - 280	lmb2st2	10.4.214.137	slot=9;subslot=0;port=13;vlanid=4061
297	Success		UoY Generic MacAuth - 280	lmb3st1	10.4.214.139	slot=2;subslot=0;port=45;vlanid=4061

MAC '74d4351aa284' Authentication Details

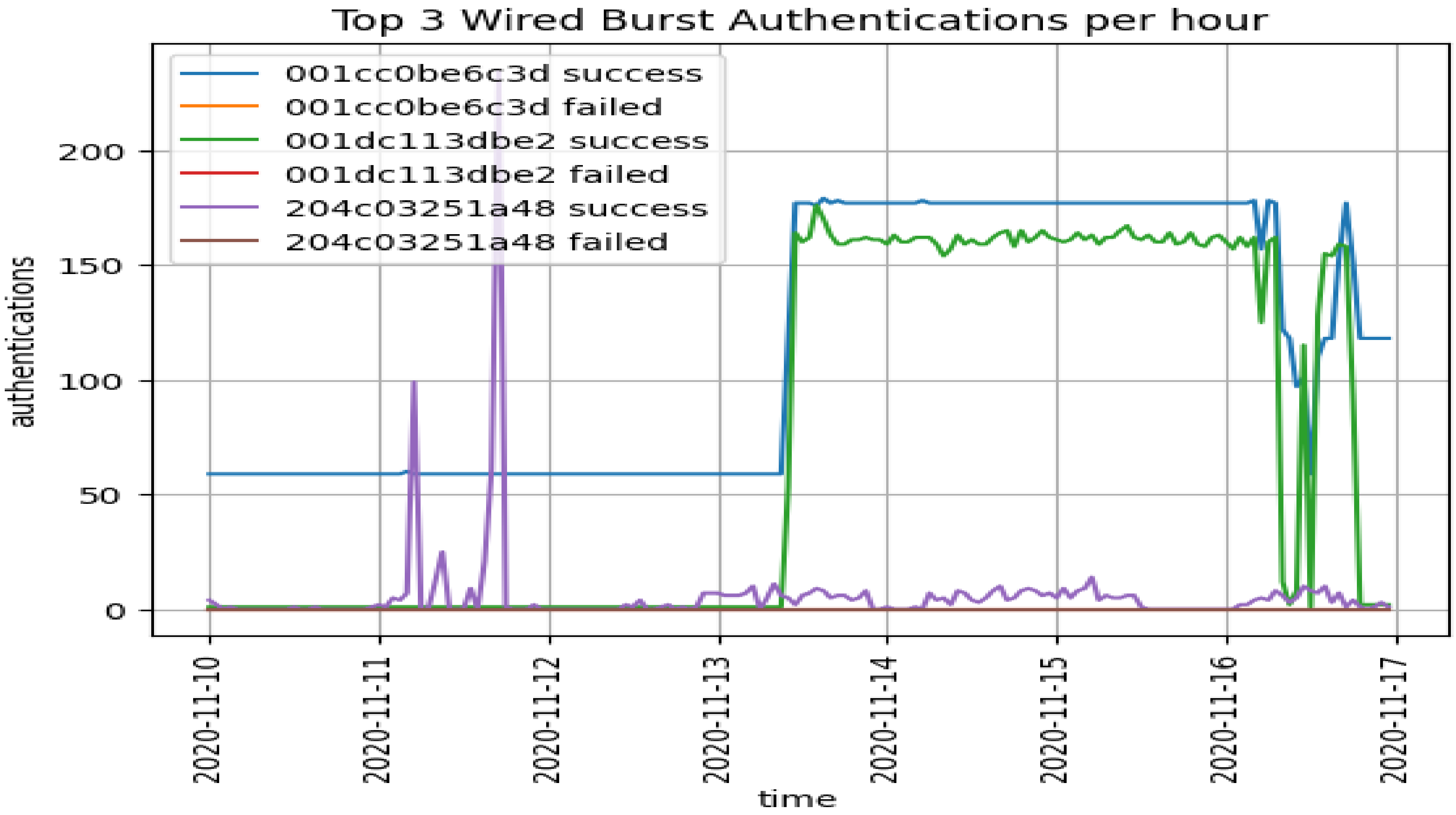
Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
9915	Success		UoY Generic MacAuth - 280	Cse1st2	10.4.48.84	slot=2;subslot=0;port=15;vlanid=3737
9208	Success		UoY Generic MacAuth - 280	rch1st3	10.4.218.85	slot=7;subslot=0;port=48;vlanid=4037
9208	Success		UoY Generic MacAuth - 280	slb1st2	10.4.228.3	slot=9;subslot=0;port=45;vlanid=3721
9208	Success		UoY Generic MacAuth - 280	pza1st2	10.4.112.2	slot=6;subslot=0;port=48;vlanid=3743
166	Success		UoY AirGroup Authorization	arubamm	144.32.76.60	

MAC '001a1e04e2b8' Authentication Details

Auths	Error	Username	Service	Switch Name	Switch IP	Switch Port
9915	Success		UoY Generic MacAuth - 280	pza1st2	10.4.112.2	slot=6;subslot=0;port=48;vlanid=3743
9915	Success		UoY Generic MacAuth - 280	slb1st2	10.4.228.3	slot=9;subslot=0;port=47;vlanid=3721
9914	Success		UoY Generic MacAuth - 280	rch1st3	10.4.218.85	slot=7;subslot=0;port=48;vlanid=4037



These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top Wireless Endpoints Authentications

NOTE: Red threshold=1750 , Amber threshold=175

Auths	Success	Failed	MAC
39203	39183	20	020000000001
21053	219	20834	0e4424e2a347
19399	0	19399	e65edcab357c
10957	118	10839	14c213cc7e78
9965	0	9965	da8ce40f849f
9960	84	9876	baf1bed1fe3a
9637	311	9326	08f69c8ac884
7667	5	7662	6cab311af526
7550	0	7550	186590324e47
7430	0	7430	1a58ed688569
7030	0	7030	c66ebca6559b
6619	0	6619	80b03db5f2dc
6462	3888	2574	78929cd1e6d8
6436	0	6436	1c5cf2dd5cfc
6389	0	6389	ccfd17fac143

These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

MAC '020000000001' Authentication Details

Auths	Error	Username	Service	NAS Name	NAS IP	SSID
19614	Success	eapoltest	UoY eapol_test TLS service - 120	sysmon0	144.32.76.5	

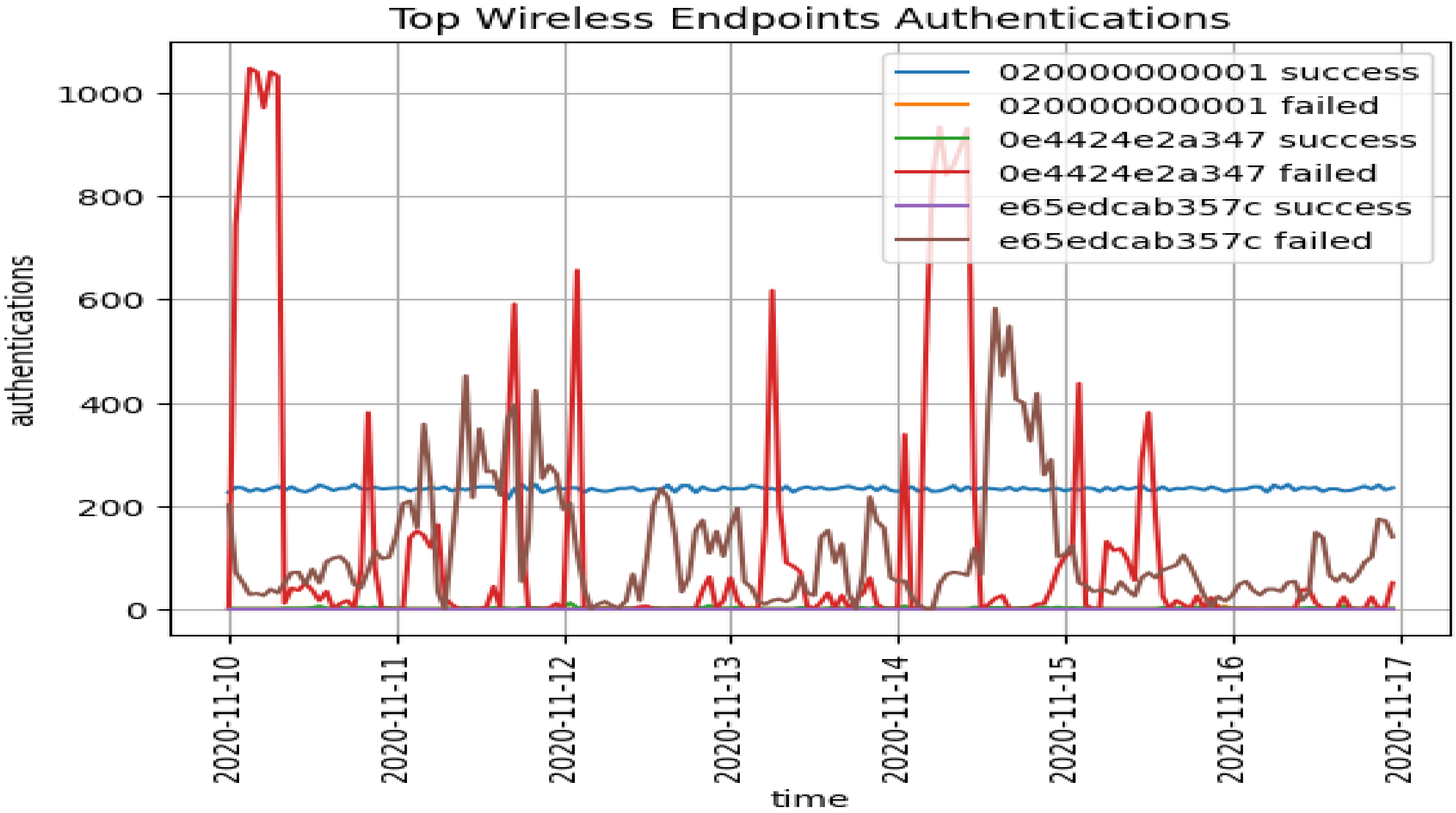
19569	Success	york.ac.uk@eduroam.ac.uk	New Eduroam Visitor Healthcheck	localhost	127.0.0.1	
19	User authentication failed	york.ac.uk@eduroam.ac.uk	New Eduroam Visitor Healthcheck	localhost	127.0.0.1	
1	No response from home s	york.ac.uk@eduroam.ac.uk	New Eduroam Visitor Healthcheck	localhost	127.0.0.1	

MAC '0e4424e2a347' Authentication Details

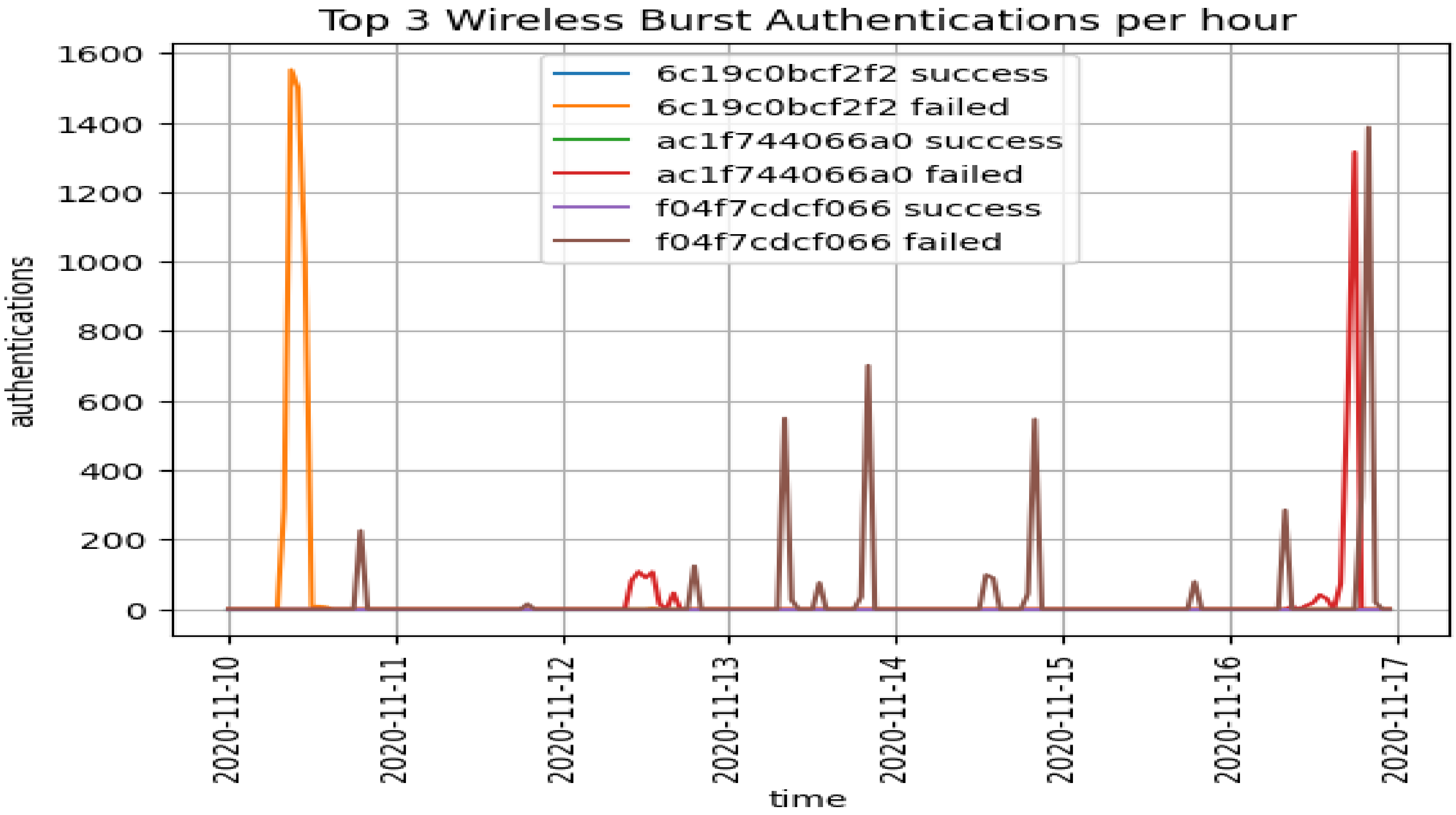
Auths	Error	Username	Service	NAS Name	NAS IP	SSID
20416	User authentication failed	Fullerton4489!	UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
321	Request timed out		UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
159	Success	vr652	UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
73	Request timed out	Fullerton4489!	UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
60	Success	vr652	UoY Eduroam Authentication - 041	arubamm	144.32.76.60	eduroam
18	User not found		UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
4	Request timed out	vr652	UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam
2	TLS session error		UoY Eduroam Authentication - 041	arubal4-vip	144.32.64.43	eduroam

MAC 'e65edcab357c' Authentication Details

Auths	Error	Username	Service	NAS Name	NAS IP	SSID
19399	User authentication failed		UoY PSK Net 140220	arubal1-vip	144.32.64.35	mydevices



These are endpoints that are typically continually attempting to connect. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top Virtual User Authentications

NOTE: Red threshold=1750 , Amber threshold=175

Auths	Success	Failed	Media	Username	Service	NAS Name	NAS IP
20709	0	20709	VPN	admin	UoY What the hell are these devic	arubal1-vip	144.32.64.35
20130	0	20130	VPN	admin	UoY What the hell are these devic	arubal4-vip	144.32.64.43
20129	0	20129	VPN	admin	UoY What the hell are these devic	arubal2-vip	144.32.64.37
20052	20052	0	VPN	arubal3	UoY Aruba Controller Authenticati	arubal3-vip	144.32.64.39
14265	0	14265	VPN	admin	UoY What the hell are these devic	aruba8dev0-coa-vip	144.32.210.71
14040	0	14040	VPN	admin	UoY What the hell are these devic	aruba8dev1-coa-vip	144.32.210.72
974	0	974	VPN	admin	UoY What the hell are these devic	bsdcfab2	10.192.0.1
806	0	806	VPN	admin	UoY What the hell are these devic	tftafab3	10.32.0.0
642	0	642	VPN	MGR	UoY What the hell are these devic	bsdcfab2	10.192.0.1
529	0	529	VPN	MGR	UoY What the hell are these devic	tftafab3	10.32.0.0
365	365	0	VPN	@hyms.ac.uk	UoY AirGroup Authorization Servic	arubamm	144.32.76.60
269	0	269	VPN	root	UoY What the hell are these devic	tftafab3	10.32.0.0
267	0	267	VPN	root	UoY What the hell are these devic	bsdcfab2	10.192.0.1
252	0	252	VPN	MANAGER	UoY What the hell are these devic	bsdcfab2	10.192.0.1
224	0	224	VPN	FIELD	UoY What the hell are these devic	bsdcfab2	10.192.0.1

Username whitelist service_radiushcheck

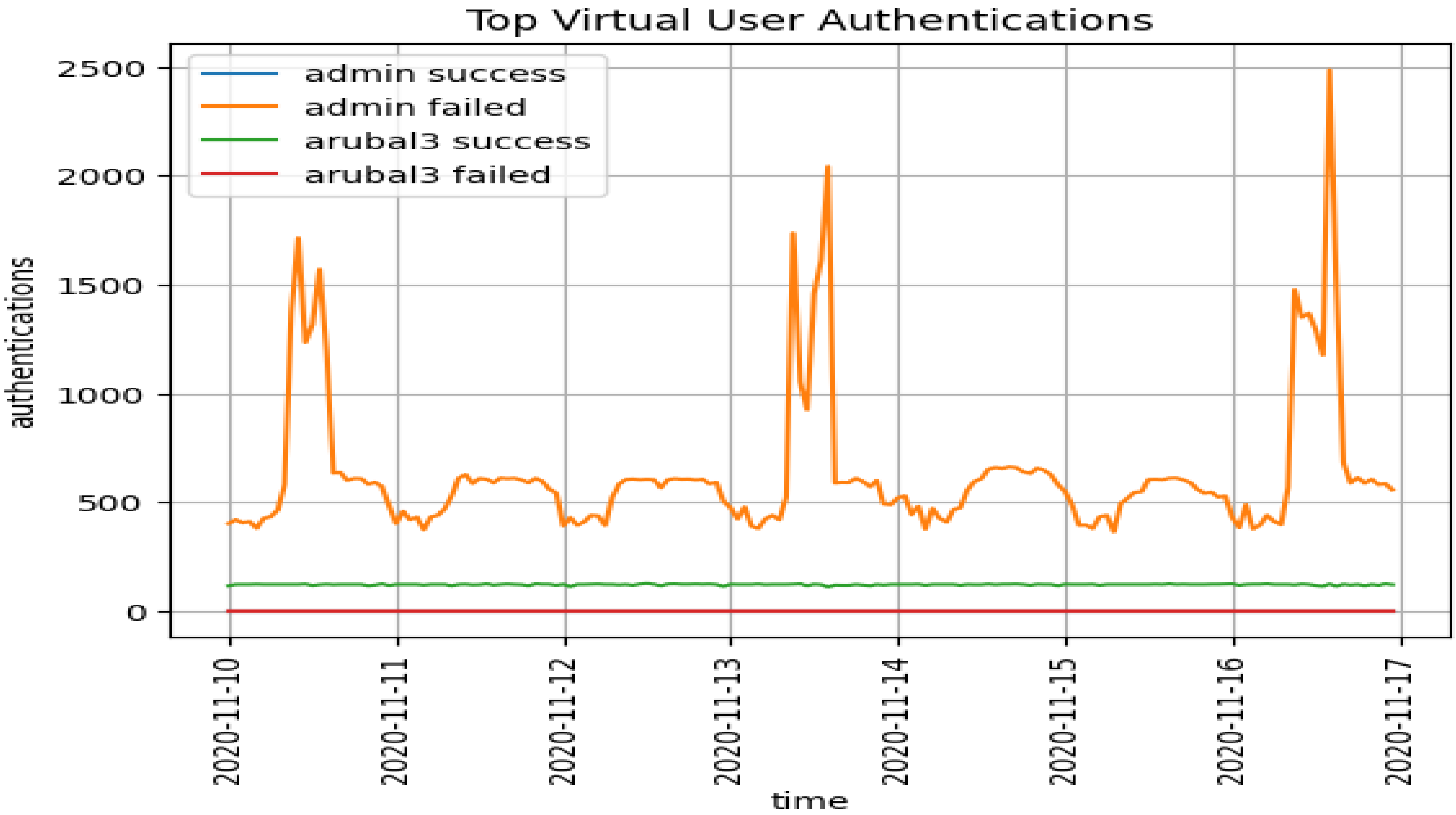
These are users that are typically using VPN or login to a system. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.

Username 'admin' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
20709	User not found	UoY What the hell are these devices - 051219	arubal1-vip	144.32.64.35
20130	User not found	UoY What the hell are these devices - 051219	arubal4-vip	144.32.64.43
20129	User not found	UoY What the hell are these devices - 051219	arubal2-vip	144.32.64.37
14265	User not found	UoY What the hell are these devices - 051219	aruba8dev0-coa-vip	144.32.210.71
14040	User not found	UoY What the hell are these devices - 051219	aruba8dev1-coa-vip	144.32.210.72
1225	User not found	UoY What the hell are these devices - 051219	bsstr0	10.192.0.9
974	User not found	UoY What the hell are these devices - 051219	bsdcfab2	10.192.0.1
875	User not found	UoY What the hell are these devices - 051219	bkbrstr0	10.192.0.8
806	User not found	UoY What the hell are these devices - 051219	tftafab3	10.32.0.0
752	User not found	UoY What the hell are these devices - 051219	ltalbrstr0	10.192.0.7
608	User not found	UoY What the hell are these devices - 051219	atbstr0	10.192.0.16
595	User not found	UoY What the hell are these devices - 051219	pbxstr0	10.192.0.12
560	User not found	UoY What the hell are these devices - 051219	pzstr0	10.192.0.6
525	User not found	UoY What the hell are these devices - 051219	envvsubstr0	10.192.0.15
455	User not found	UoY What the hell are these devices - 051219	tftastr1	10.192.0.24

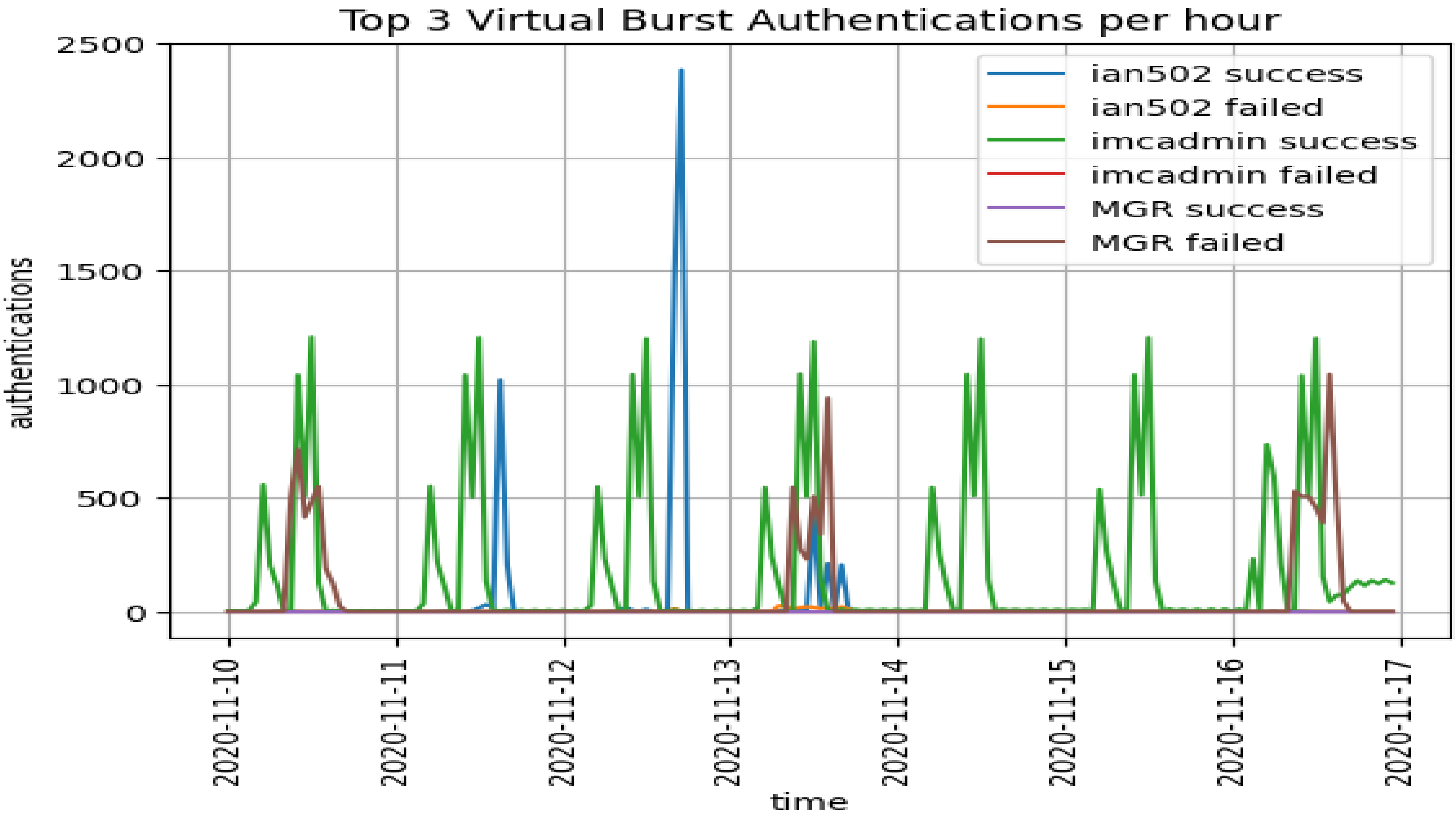
Username 'arubal3' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
20052	Success	UoY Aruba Controller Authentication - 140217	arubal3-vip	144.32.64.39



User whitelist service_radiushcheck

These are users that are typically using VPN or login to a system. Connection Threshold can be set, this will highlight device in red - these should be investigated. Amber are one tenth the red.



User whitelist service_radiushcheck

This graph highlights endpoints that have burst of excessive authentication. These devices should be investigated.

Top 15 802.1X Users Authentications

NOTE: Red threshold=2100 , Amber threshold=210

Auths	Success	Failed	User
4495390	4494813	577	service_radiushcheck
20489	0	20489	Fullerton4489!
20189	20023	166	envr529
19614	19614	0	eapoltest
11473	0	11473	jp1807
10480	0	10480	Uyipcislife1
10442	9340	1102	secure01
9275	0	9275	Jasper10
8612	8534	78	km1547
7009	196	6813	lom510
6498	119	6379	lcsd502
6088	6068	20	cape
5934	5785	149	admn622
5918	3888	2030	info-display-5F69@york.ac.uk
5357	5172	185	eln519

This highlight specific 802.1X user authentications. Connection Threshold can be set, this will highlight users in red - these should be investigated. Amber are one tenth the red.

Username 'service_radiushcheck' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
181442	Success	UoY Health-Check - 280319	lb2-222	144.32.222.40

181438	Success	UoY Health-Check - 280319	lb3-222	144.32.222.36
60478	Success	UoY Health-Check - 280319	ce1sta2	10.4.55.47
30281	Success	UoY Health-Check - 280319	gsha1sta1	10.4.200.2
30267	Success	UoY Health-Check - 280319	gdia1sta1	10.4.200.19
30259	Success	UoY Health-Check - 280319	jl1sta1	10.4.77.5
30255	Success	UoY Health-Check - 280319	gdia2sta1	10.4.200.20
30252	Success	UoY Health-Check - 280319	gshb1sta1	10.4.200.4
30243	Success	UoY Health-Check - 280319	jm1sta1	10.4.77.9
30242	Success	UoY Health-Check - 280319	gsha2sta1	10.4.200.3
30240	Success	UoY Health-Check - 280319	g010swa1	10.4.75.81
30240	Success	UoY Health-Check - 280319	atb057swa1	10.4.100.205
30240	Success	UoY Health-Check - 280319	g001swa1	10.4.75.79
30240	Success	UoY Health-Check - 280319	aew004swa1	10.4.100.203
30240	Success	UoY Health-Check - 280319	dl002swa1	10.4.59.98

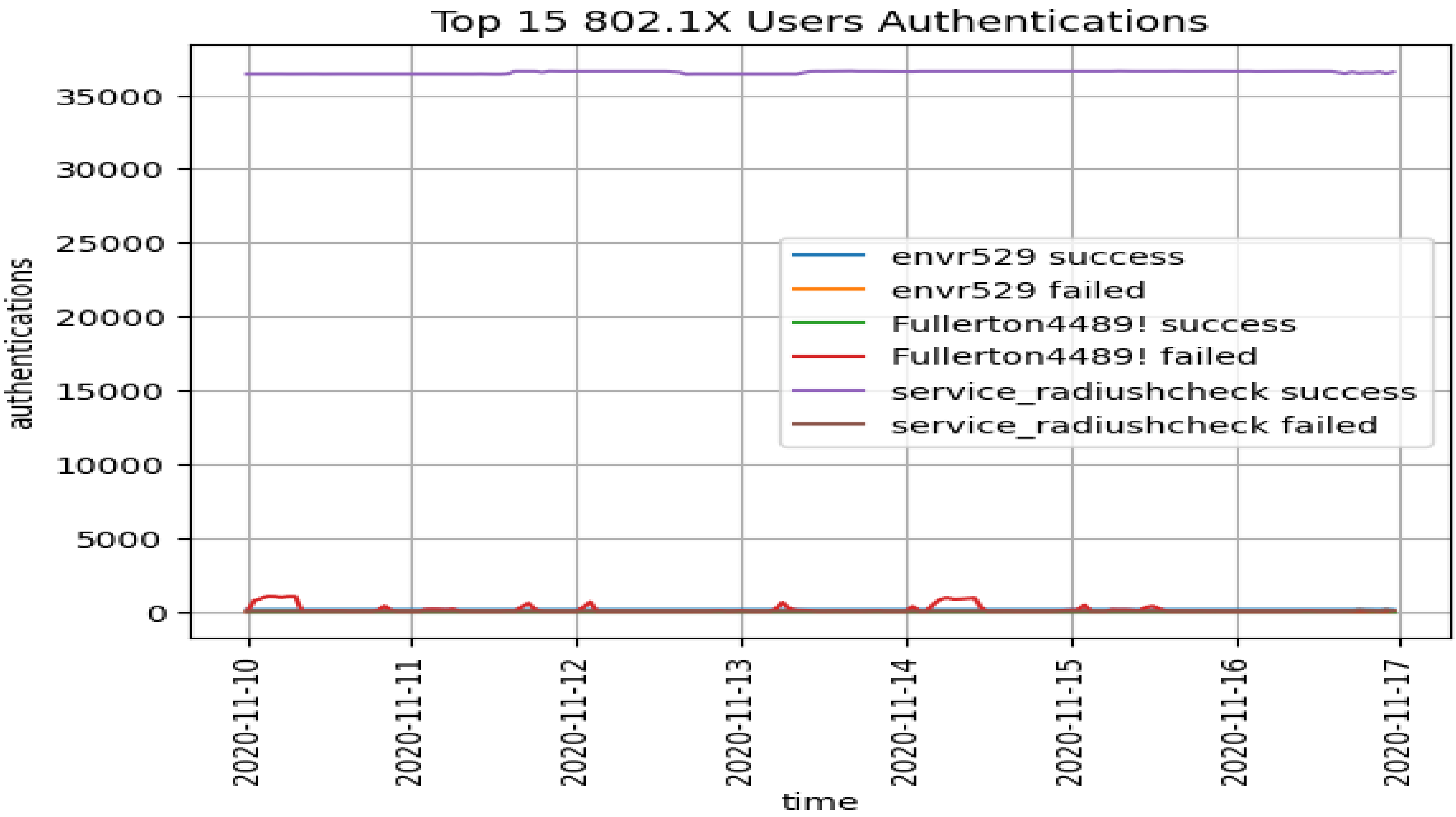
Username 'Fullerton4489!' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
20416	User authentication failed	UoY Eduroam Authentication - 041219	arubal4-vip	144.32.64.43
73	Request timed out	UoY Eduroam Authentication - 041219	arubal4-vip	144.32.64.43

Username 'envr529' Authentication Details

Auths	Error	Service	NAS Name	NAS IP
14990	Success	UoY Eduroam Authentication - 041219	arubal3-vip	144.32.64.39
5033	Success	UoY Eduroam Authentication - 041219	arubal4-vip	144.32.64.43
213	Request timed out	UoY Eduroam Authentication - 041219	arubal3-vip	144.32.64.39

13	Request timed out	UoY Eduroam Authentication - 041219	arubal4-vip	144.32.64.43



This highlight specific 802.1X user authentications. Connection Threshold can be set, this will highlight users in red - these should be investigated. Amber are one tenth the red.

Top 15 NAS with Most Authentications

NOTE: Red threshold=7000 , Amber threshold=700

Media	Auths	Success	Failed	NAS Name	NAS IP
Wired	328644	328641	3	pc001st1	10.4.9.126
Wired	217226	217223	3	bk1st1	10.4.204.43
Wired	205608	205608	0	psyc3st1	10.4.87.8
Wired	195501	195497	4	bk1st2	10.4.204.44
Wired	159722	159722	0	pt405st1	10.4.9.52
Wired	150205	150203	2	psyc2st1	10.4.87.7
Wired	138363	138363	0	innovuoyst1	10.4.63.42
Wired	131682	131682	0	bh1st1	10.4.204.106
Wired	131290	131286	4	wn1st2	10.4.73.153
Wired	129946	129946	0	g1st1	10.4.75.49
Wired	117439	117439	0	Cse2st2	10.4.48.86
Wired	110928	110928	0	bioc1sta1	10.4.63.8
Wired	110406	110406	0	pt205st1	10.4.9.53
Wired	101397	101397	0	lmb3st1	10.4.214.139
Wired	100756	100756	0	lce1sw2	10.4.210.14

These highlights the NAS that are the source of most authentications. Typically, you would expect the wireless concentrators to be at the top. To appreciate these will likely require longer monitoring of the environment, though a NAS with excessive authentications will stand out - these should be investigated.

Top 10 NAS with Least Authentications

Media	Auths	Success	Failed	NAS Name	NAS IP

Wired	3	3	0	k173sw0	10.4.220.16
Wired	3	3	0	hxgw2sw1	10.4.97.55
Wired	3	3	0	jx1sw0	10.4.77.253
Wired	4	4	0	vchsw0	144.32.242.84
Wired	6	6	0	hxgw1sw1	10.4.97.54
Wired	7	7	0	gdium1sw0	10.4.200.122
Wired	7	7	0	dum1sw0	10.4.44.148
Wired	7	7	0	nslcsum1sw0	10.4.100.17
Wired	7	7	0	dum2sw0	10.4.89.43
Wired	7	7	0	aum1sw0	10.4.100.196

This might be useful to see if there is any equipment that can be decommissioned. WARNING: This does not report the NAS that have had no authentications! This can be got by interrogating the tipsdb directly.

Top 15 Failed Authorization

NOTE: Red threshold=350 , Amber threshold=35

Authz	Username	MAC	Service	Method	NAS	NAS IP	Media	Port/SSID
1764	asw555	70ea5a6c981e	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
877	cmd7	9017c81fd454	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
580	jj1254	00be3b3de236	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
409	am2697	542b8d6f3f90	UoY Block invalid edur	EAP-PEAP(EAP-	arubal4-vip	144.32.64.43	Wifi	eduroam
207	ew1368	2a471f841443	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
196	ky753	d88adca638d1	UoY Block invalid edur	EAP-PEAP(EAP-	arubal4-vip	144.32.64.43	Wifi	eduroam
174	yz4923	ceb4ab49b2fe	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
143		38f9d30aaf2f	UoY ArubaAP Wired P	MAC-AUTH	arubal1-vip	144.32.64.35	Wired	1.1.1.11:0/2
98	zld100	c6b9ea6237cc	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
91	tel506@york.ac.uk	46b670587a2c	UoY Eduroam Authent	EAP		arubal4-vip	144.32.64.43	Wifi	eduroam
74	hnf502	129a452dc309	UoY Block invalid edur	EAP-PEAP(EAP-	arubal4-vip	144.32.64.43	Wifi	eduroam
68		34e6d718e362	UoY ArubaAP Wired P	MAC-AUTH	arubal2-vip	144.32.64.37	Wired	10.4.226.151:0/1
67	gf743	04d395123333	UoY Block invalid edur	EAP-PEAP(EAP-	arubal3-vip	144.32.64.39	Wifi	eduroam
58	hh1245	a4933fe1d374	UoY Block invalid edur	EAP-PEAP(EAP-	arubal2-vip	144.32.64.37	Wifi	eduroam
52		0009dff3cd90	UoY ArubaAP Wired P	MAC-AUTH	arubal1-vip	144.32.64.35	Wired	10.4.226.237:0/1

These are authentication requests that were successful but the authorization failed the request. Excessive failures should be investigated to understand what is wrong.

Top 10 802.1X Users with Multiple Devices

NOTE: Red threshold=105 , Amber threshold=10

Devices	Username
630	td923
189	service_radiushcheck
20	hyms509
18	pn664
17	alc618
17	hyms515
13	admn622
12	hp1018
11	tjgl500
11	pmj516

These highlights users that are authenticating from multiple devices. It then identifies the top 3 users and their associated devices.

Top 10 802.1X Devices with Multiple Users

NOTE: Red threshold=105 , Amber threshold=10

Users	MAC
5	94e6f77cfb64
4	7cb27d0ceebe
3	40f02fa95737
3	f8ac652bc302
3	f8ac652bc352
3	f8ac6556bb93
3	f8ac655b2241
3	f8ac655bc1d8
3	f8ac655bc949
3	f8ac655bc9ad

These highlights shared devices.

Top 10 Wired Devices that have Moved

NOTE: Red threshold=28 , Amber threshold=2

Moves	MAC
8	001dc111d166
8	bcc34288983f
7	000c92f079e1
7	000c92f07a2c
7	001a1e04e198
7	001dc10fe60c
7	001dc1125d28
7	001dc113dbe2
7	00609f9438ae
7	00609f951f2c

These highlights wired devices that have physically been moved to different wired ports. It then identifies the top 3 devices and where they moved.

Top 10 Wireless Devices with Multiple SSID

NOTE: Red threshold=28 , Amber threshold=2

SSID moves	MAC
2	04d6aa7c7500
2	2c261790cd2c
2	a0d807fa1cc2
2	d8c0a633afb1
2	e0accb99d224
2	f6d017073124

These highlights devices that are moving between different SSIDs.

Top 15 TACACS Authentications

NOTE: Red threshold=700 , Amber threshold=70

Username	Source	Destination	Auths	Success	Failed
admin	144.32.128.94	127.0.0.1	35	0	35
MGR	144.32.128.94	127.0.0.1	11	0	11
emm502	144.32.226.117	127.0.0.1	10	10	0
pkp506	144.32.226.181	127.0.0.1	10	10	0
ian502	172.18.6.2	127.0.0.1	8	8	0
FIELD	144.32.128.94	127.0.0.1	8	0	8
ian502	144.32.226.97	127.0.0.1	7	6	1
MANAGER	144.32.128.94	127.0.0.1	7	0	7
as1558	172.18.6.8	127.0.0.1	6	6	0
MAIL	144.32.128.94	127.0.0.1	5	0	5
cdn1	144.32.226.185	127.0.0.1	4	4	0
HELLO	144.32.128.94	127.0.0.1	4	0	4
pkp506	10.241.18.161	127.0.0.1	4	4	0
emm502	10.240.150.218	127.0.0.1	4	4	0
maint	144.32.128.94	127.0.0.1	4	0	4

These highlights users generating excessive TACACS authentications. These might be legitimate. WHITELIST? Connection Threshold can be set, this will highlight user in red - these should be investigated. Of these the ones in red will be drilled into more detail.

Top 15 Device Session Duration

NOTE: Red duration=100 days, Amber duration=10 days

MAC	**Username**	**Days**	In_GBytes	Out_GBytes	Total_GBytes	Device Type
001ae8a963fa		**203**	0.000	0.000	0.000	VoIP Phone
001ae87a852b		**201**	0.000	0.000	0.000	VoIP Phone
001ae878a2c8		**201**	0.000	0.000	0.000	VoIP Phone
00d02df37c2d		**201**	0.000	0.000	0.000	*Not Known*
001ae87a82e9		**201**	0.000	0.000	0.000	VoIP Phone
001ae878a331		**201**	0.000	0.000	0.000	VoIP Phone
001ae8755dbd		**199**	0.000	0.000	0.000	VoIP Phone
001ae8755d7e		**199**	0.000	0.000	0.000	VoIP Phone
001ae8755de1		**199**	0.000	0.000	0.000	VoIP Phone
001ae875267e		**199**	0.000	0.000	0.000	VoIP Phone
001ae875306e		**199**	0.000	0.000	0.000	VoIP Phone
001ae8755b28		**199**	0.000	0.000	0.000	VoIP Phone
001ae8654728		**199**	0.000	0.000	0.000	VoIP Phone
001ae854e17d		**199**	0.000	0.000	0.000	VoIP Phone
001ae87527ce		**199**	0.000	0.000	0.000	VoIP Phone

This reports the sessions with the longest duration. This information is supplied by the NAS within the RADIUS Accounting - sometime this my report preposterous information - this is an error of the NAS. Questions is are these top session durations reasonable?

Top 15 Device Session Total Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	**Username**	**Days**	**In_GBytes**	**Out_GBytes**	**Total_GBytes**	Device Category
0090aa0734bb		0	5579	146	**5725**	*Not Known*
0090aa07350b		0	5476	144	**5620**	*Not Known*
0090aa072f57		0	4584	134	**4718**	*Not Known*
0090aa073468		0	3165	78	**3243**	*Not Known*
0090aa0b5f7f		0	2045	47	**2093**	*Not Known*
0c9d9265cd08		0	1919	63	**1982**	Computer
c03ebacabb69		0	78	1273	**1351**	*Not Known*
0090aa072aa9		0	1157	33	**1189**	*Not Known*
0090aa07340c		0	1079	29	**1108**	*Not Known*
40167ea4ba04		0	318	357	**675**	Computer
e82689cc0634		0	13	446	**459**	Access Points
2c4d544336ab		0	149	182	**331**	Computer
3024a90d917f		0	0	315	**315**	Network Boot Agents
6045cba3eb35		0	73	216	**288**	Computer
a823fea7231c		0	4	283	**287**	Home Audio/Video Equipment

This reports the combination the device's ingress and egress traffic averaged over a per day basis.

Top 15 Device Session Transmit Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	**Username**	**Days**	**In_GBytes**	**Out_GBytes**	Total_GBytes	Device Category
c03ebacabb69		0	78	**1273**	1351	*Not Known*
e82689cc0634		0	13	**446**	459	Access Points
40167ea4ba04		0	318	**357**	675	Computer
3024a90d917f		0	0	**315**	315	Network Boot Agents
a823fea7231c		0	4	**283**	287	Home Audio/Video Equipment
40167ea45f9c		0	6	**229**	235	Computer
6045cba3eb35		0	73	**216**	288	Computer
0009dff3c44f		0	51	**207**	258	Home Audio/Video Equipment
a8a159278990	eb1832@york.ac.uk	1	34	**190**	224	Computer
2c4d544336ab		0	149	**182**	331	Computer
00d86156dfe7	cmr544@york.ac.uk	1	4	**157**	160	Computer
0090aa0734bb		0	5579	**146**	5725	*Not Known*
0090aa07350b		0	5476	**144**	5620	*Not Known*
2cf05d0644d7	amb633@york.ac.uk	1	7	**141**	148	Computer
0c9d92bfba67		0	73	**139**	212	Computer

This reports the combination the device's egress traffic averaged over a per day basis.

Top 15 Device Session Receive Data Average per Day

NOTE: Red threshold=10 , Amber threshold=1

MAC	**Username**	**Days**	**In_GBytes**	Out_GBytes	Total_GBytes	Device Category
0090aa0734bb		0	**5579**	146	5725	*Not Known*
0090aa07350b		0	**5476**	144	5620	*Not Known*
0090aa072f57		0	**4584**	134	4718	*Not Known*
0090aa073468		0	**3165**	78	3243	*Not Known*
0090aa0b5f7f		0	**2045**	47	2093	*Not Known*
0c9d9265cd08		0	**1919**	63	1982	Computer
0090aa072aa9		0	**1157**	33	1189	*Not Known*
0090aa07340c		0	**1079**	29	1108	*Not Known*
40167ea4ba04		0	**318**	357	675	Computer
2c4d544336ab		0	**149**	182	331	Computer
0090aa02ee35		0	**133**	4	138	*Not Known*
0090aa072b29		0	**124**	4	128	*Not Known*
0090aa072a7e		0	**91**	3	93	*Not Known*
1831bf2d6bac		0	**89**	57	145	Computer
c03ebacabb69		0	**78**	1273	1351	*Not Known*

This reports the combination the device's ingress traffic averaged over a per day basis.

ClearPass Audit

This reports the last 15 changes.

Time	User	Category	Action	Change
2020-11-10 12:32:16+00:00	dam6	Network Device	ADD	vchswa1
2020-11-10 12:32:37+00:00	dam6	Device Group	MODIFY	HP&#x28;ArubaOS&#x29;
2020-11-10 12:32:57+00:00	dam6	Device Group	MODIFY	HP &#x28;Procurve&#x29;
2020-11-10 13:15:51+00:00	jw3322	Guest User	ADD	501ac5be29c9
2020-11-10 14:11:30+00:00	jdc560	Guest User	ADD	1c1adf81bbaa
2020-11-10 14:15:20+00:00	jdc560	Guest User	REMOVE	1c1adf81bbaa
2020-11-10 14:15:38+00:00	aeh607	Guest User	ADD	f8461cf71321
2020-11-10 14:19:07+00:00	jdc560	Guest User	ADD	1c1adf81bbaa
2020-11-10 14:19:30+00:00	jdc560	Guest User	MODIFY	1c1adf81bbaa
2020-11-10 14:40:45+00:00	cma527	Guest User	ADD	e4f04240b092
2020-11-10 14:42:21+00:00	cma527	Guest User	REMOVE	e4f04240b092
2020-11-10 15:47:29+00:00	wo541	Guest User	ADD	a085fc268874
2020-11-10 15:51:36+00:00	wo541	Guest User	REMOVE	a085fc268874
2020-11-10 15:52:21+00:00	wo541	Guest User	ADD	a085fc268874
2020-11-10 16:07:52+00:00	je851	Guest User	ADD	00e04c785737

OnGuard Summary

Total	Unknown	Infected	Healthy	Checkup	Quarantine	Transition	No Status
5329	2245	0	0	0	0	0	0

Reports the current state of all the OnGuard clients.

10 Most Recent OnGuard Posture Failures

Date	MAC	IP	Hostname	Username	OS

This reports the PCs that have most recently failed their posture compliance. The highlighted section shows what the failed component has - not what it failed against!