BEST PRACTICES FOR APPROPRIATE USE OF LOGGER.

With Serguei Esquivel

Session agenda

1. Why EPS impact performance?
2. Understanding storage.
3. Backup and upgrade.
4. Certificate Management.
5. Login Methods.
6. Q&A.

Why EPS impact performance

What is an event?

""",-
9223372036854775808,-9223372036854775808,""",-9223372036854775808,-2147483648,-
2147483648,OA9S-jgBABCAJ6RNIm8-nQ==vianney-pc.americas.hpqcorp.net,275238529,-
9223372036854775808,-9223372036854775808,""",/All Zones/ArcSight System/Public Address Space Zones/Digital Equipment
Corporation,""",""",""",""",""",""",""",5.2.4.0.0,America/Los_Angeles,3sM1R-jgBABCAAqRNIm8-
nQ==,aixauditpr_filevianney-PC,2130706433,-9223372036854775808,-
9223372036854775808,""",/All Zones/ArcSight System/Private Address Space Zones/Local Network Zones/RFC5735: IANA - Loopback (127.0.0.0-
127.255.255.255),""",""",""",""",""",""",""",5.2.4.0.0,America/Los_Angeles,""",ArcSight,ArcSight,""",
""",""","""""""""""""""""",""",""",""",""",""",Security
Mangement,""",""""/home/vianney/Code/Perforce/vianney-
uPC/feature/typhoon/agent/vboncorps/test/gate/data/agent/aixauditpr_file/test/aix-audit-
log.txt,""",""",""",-9223372036854775808,-9223372036854775808,-
9223372036854775808,""","""""""""""

StreamHeaderTypeCounts,1SecurityEvent,614,-128,""",Operating System: [Linux 2.4.18 -
2.4.20],""",0,1113005083000,1113005083000,-9223372036854775808,""","","","","","",-
9223372036854775808,-2147483648,-2147483648,""","","","","","","",-2147483648,-2147483648,-
2147483648,-2147483648,-2147483648,0,1113599506843,""","","",1113005083000,""","","",-
2147483648,0,1,""","","","","","","","",-9223372036854775808,-9223372036854775808,-
9223372036854775808,-9223372036854775808,-9223372036854775808,""","","","","","",-
9223372036854775808,-9223372036854775808,""",-9223372036854775808,-2147483648,-2147483648,m-
mzRwMBABCACLvX01HtFw==gmanlaptop,3232256026,-9223372036854775808,-9223372036854775808,""",/All
Zones/System Zones/Private Address Space/RFC1918: 192.168.0.0-
192.168.255.255,""","","","","","","",3.1.0.0.0,America/Los_Angeles,3gqqzRwMBABC5vjDRIb-
FqQ==,ncircle_scanner""",-9223372036854775808,-9223372036854775808,-
9223372036854775808,""","","","","","","","","","",America/Los_Angeles,""",nCircle,Vulnerability
Scanner,""","","","""""""""""""""""""""""""",""",/scanner/device/uri,""","","","","""""""",/Site Asset Categories/Operating
System/Linux/2.4.18 - 2.4.20,""","",-9223372036854775808,-9223372036854775808,-
9223372036854775808,""","""""""""""""doucemere.sv.arcsight.com,3232240673,-9223372036854775808,-
9223372036854775808,""",/All Zones/System Zones/Private Address Space/RFC1918: 192.168.0.0-
192.168.255.255,""","","","","","","",-2147483648,-2147483648,""","","","","""""""""""""""

StreamHeaderTypeCounts,1SecurityEvent,61""",-128,""",Agent [ibm_nsa584116062202] type [ibm_nsa] started,""",0,1140655329093,1140655329093,1140655329175,""",""",""",""",InternalAlertSender[31CtflAkBABCs8iDyfTk-2w==],""",-9223372036854775808,-2147483648,-2147483648,""",""",""",""",""",""",""",-2147483648,-2147483648,-2147483648,-2147483648,1,1140655329220,/Agent/Started,Warning,""",1140655329093,agent:030,""",""",-2147483648,0,1,""",""",\LResource ID="31CtflAkBABCs8iDyfTk-2w==/\G,""",""",""",""",-9223372036854775808,-9223372036854775808,-9223372036854775808,-9223372036854775808,-9223372036854775808,""",""",""",""",""",""",-9223372036854775808,-9223372036854775808,""",-9223372036854775808,-2147483648,-2147483648,xA9blAkBABCACTpbdQMUPQ==cheddar.qa.arcsight.com,-9223372036854775808,-9223372036854775808,-9223372036854775808,""",""",""",""",""",""",""",""",""",3.5.1.3800.0,America/Los_Angeles,31CtflAkBABCs8iDyfTk-2w==,ibm_nsacheddar.qa.arcsight.com,2130706433,-9223372036854775808,-9223372036854775808,""",/All Zones/System Zones/RFC1700,""",""",""",""",""",""",""",3.5.1.3800.0,America/Los_Angeles,""",ArcSight,ArcSight,""",""",""",""""""""

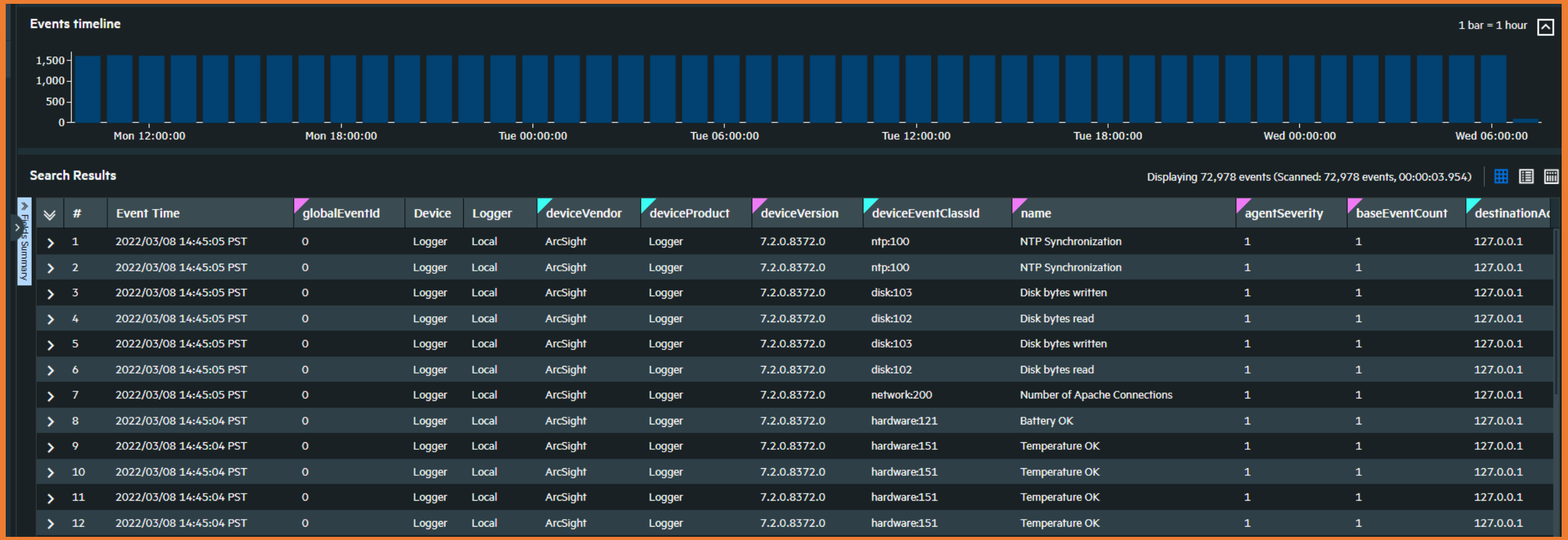
- Microsoft event: 20MB ~ 200MB
- Cisco event: ~ 600B

Questions?

Understanding storage.

Receivers

- There is no limitation on the number or type of receivers, or its maximum throughput.
- However, adding more than 40 to 50 receivers may affect performance. A high incoming event
- rate and large event size can affect the performance of a receiver. The recommended
- maximum total events per second (EPS) incoming rate is 15K. The connectors that send events
- to the Logger may have limits on their throughput.



#	Event Time	globalEventId	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId	name	agentSeverity	baseEventCount	destinationAd
1	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	ntp:100	NTP Synchronization	1	1	127.0.0.1
2	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	ntp:100	NTP Synchronization	1	1	127.0.0.1
3	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	disk:103	Disk bytes written	1	1	127.0.0.1
4	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	disk:102	Disk bytes read	1	1	127.0.0.1
5	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	disk:103	Disk bytes written	1	1	127.0.0.1
6	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	disk:102	Disk bytes read	1	1	127.0.0.1
7	2022/03/08 14:45:05 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	network:200	Number of Apache Connections	1	1	127.0.0.1
8	2022/03/08 14:45:04 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	hardware:121	Battery OK	1	1	127.0.0.1
9	2022/03/08 14:45:04 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	hardware:151	Temperature OK	1	1	127.0.0.1
10	2022/03/08 14:45:04 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	hardware:151	Temperature OK	1	1	127.0.0.1
11	2022/03/08 14:45:04 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	hardware:151	Temperature OK	1	1	127.0.0.1
12	2022/03/08 14:45:04 PST	0	Logger	Local	ArcSight	Logger	7.2.0.8372.0	hardware:151	Temperature OK	1	1	127.0.0.1

```
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_10
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_11
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_12
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_13
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_14
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_15
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_16
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_17
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_18
```

Best Practices

- Set Storage Volume
- Set Storage Group
- Set Storage Rules

Questions?

Backup and Upgrade

What is a backup?

Archives / Backup Configuration

```
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_10
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_11
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_12
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_13
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_14
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_15
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_16
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_17
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_18
```

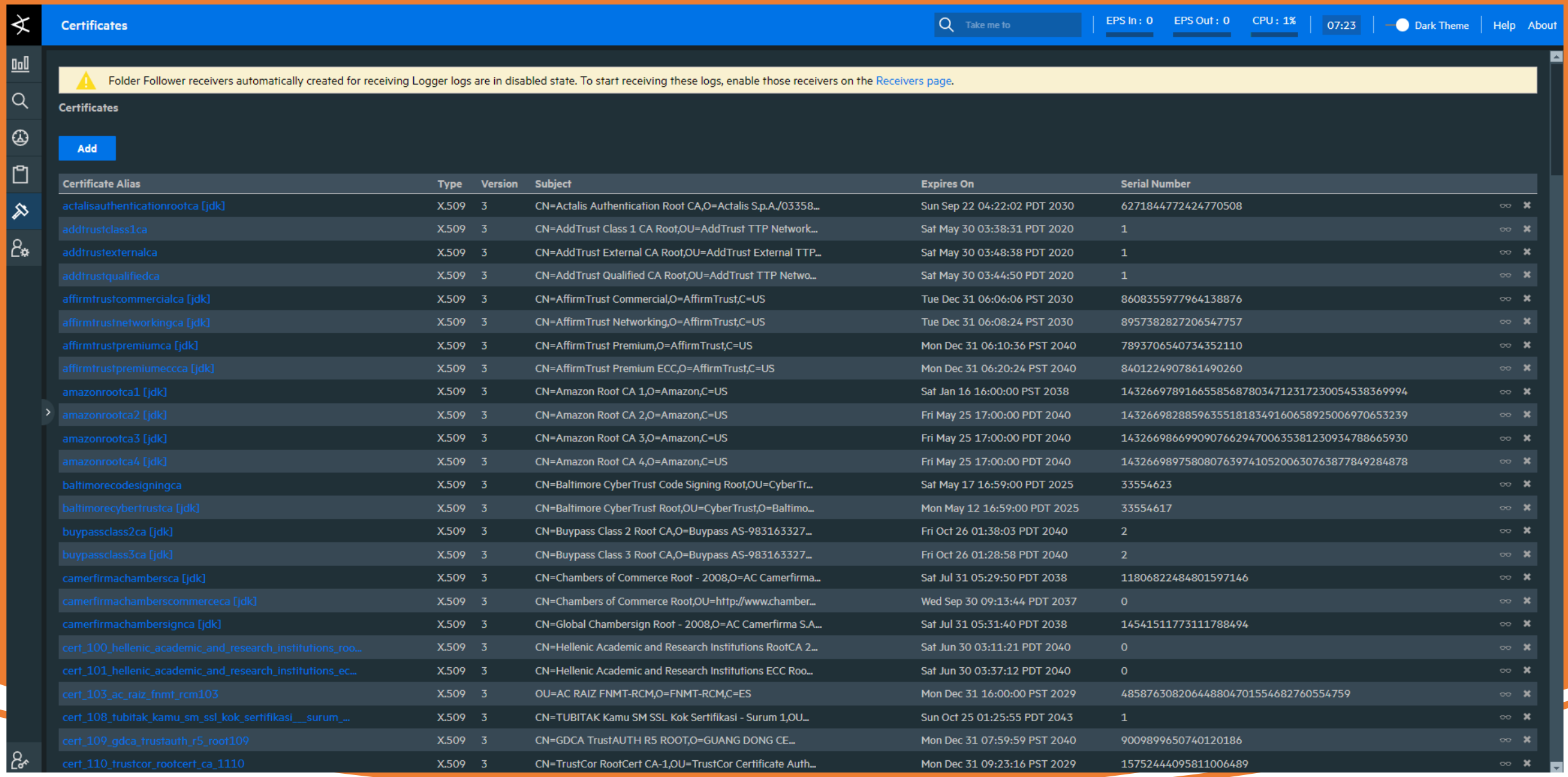
Archives:

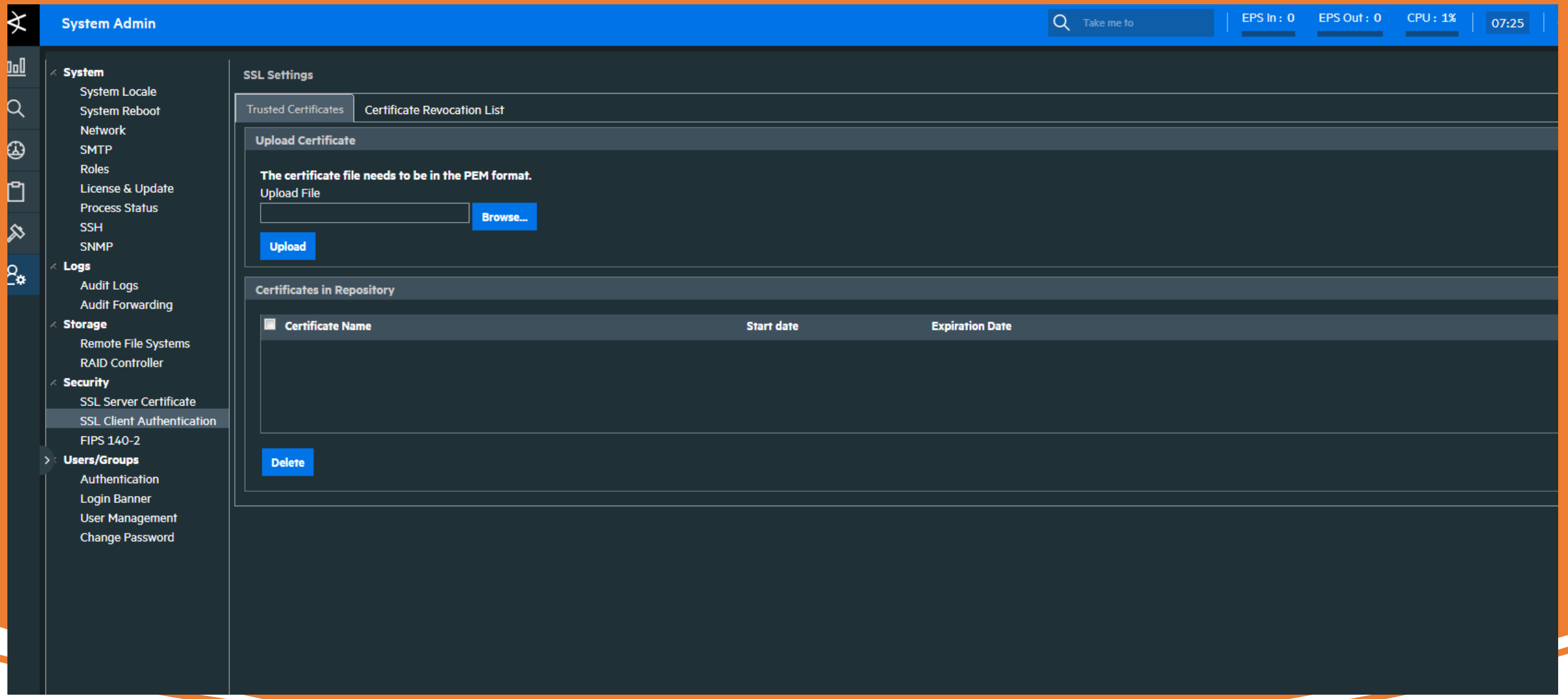
- NFS
- SMB/CIFS

```
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_10
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_11
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_12
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_13
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_14
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_15
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_16
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_17
-rw-------. 1 arcsight arcsight      0 Mar  7 09:22 Arcsight_Data_18
```

Questions?

Certificate Management


Certificates
Take me to
EPS In : 0
EPS Out : 0
CPU : 1%
07:23
Dark Theme
Help
About
Folder Follower receivers automatically created for receiving Logger logs are in disabled state. To start receiving these logs, enable those receivers on the Receivers page.
Certificates
Add
Certificate Alias | Type | Version | Subject | Expires On | Serial Number
actalisauthenticationrootca [jdk] | X.509 | 3 | CN=Actalis Authentication Root CA,O=Actalis S.p.A./03358... | Sun Sep 22 04:22:02 PDT 2030 | 6271844772424770508
addtrustclass1ca | X.509 | 3 | CN=AddTrust Class 1 CA Root,OU=AddTrust TTP Network... | Sat May 30 03:38:31 PDT 2020 | 1
addtrustexternalca | X.509 | 3 | CN=AddTrust External CA Root,OU=AddTrust External TTP... | Sat May 30 03:48:38 PDT 2020 | 1
addtrustqualifiedca | X.509 | 3 | CN=AddTrust Qualified CA Root,OU=AddTrust TTP Netwo... | Sat May 30 03:44:50 PDT 2020 | 1
affirmtrustcommercialca [jdk] | X.509 | 3 | CN=AffirmTrust Commercial,O=AffirmTrust,C=US | Tue Dec 31 06:06:06 PST 2030 | 8608355977964138876
affirmtrustnetworkingca [jdk] | X.509 | 3 | CN=AffirmTrust Networking,O=AffirmTrust,C=US | Tue Dec 31 06:08:24 PST 2030 | 8957382827206547757
affirmtrustpremiumca [jdk] | X.509 | 3 | CN=AffirmTrust Premium,O=AffirmTrust,C=US | Mon Dec 31 06:10:36 PST 2040 | 7893706540734352110
affirmtrustpremiumeccca [jdk] | X.509 | 3 | CN=AffirmTrust Premium ECC,O=AffirmTrust,C=US | Mon Dec 31 06:20:24 PST 2040 | 8401224907861490260
amazonrootca1 [jdk] | X.509 | 3 | CN=Amazon Root CA 1,O=Amazon,C=US | Sat Jan 16 16:00:00 PST 2038 | 1432669789166558568780347123172300545383699 94
amazonrootca2 [jdk] | X.509 | 3 | CN=Amazon Root CA 2,O=Amazon,C=US | Fri May 25 17:00:00 PDT 2040 | 1432669828859635518183491606589250069706532 39
amazonrootca3 [jdk] | X.509 | 3 | CN=Amazon Root CA 3,O=Amazon,C=US | Fri May 25 17:00:00 PDT 2040 | 1432669866990907662947006353812309347886659 30
amazonrootca4 [jdk] | X.509 | 3 | CN=Amazon Root CA 4,O=Amazon,C=US | Fri May 25 17:00:00 PDT 2040 | 1432669897580807639741052006307638778492848 78
baltimorecodesigningca | X.509 | 3 | CN=Baltimore CyberTrust Code Signing Root,OU=CyberTr... | Sat May 17 16:59:00 PDT 2025 | 33554623
baltimorecybertrustca [jdk] | X.509 | 3 | CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimo... | Mon May 12 16:59:00 PDT 2025 | 33554617
buypassclass2ca [jdk] | X.509 | 3 | CN=Buypass Class 2 Root CA,O=Buypass AS-983163327... | Fri Oct 26 01:38:03 PDT 2040 | 2
buypassclass3ca [jdk] | X.509 | 3 | CN=Buypass Class 3 Root CA,O=Buypass AS-983163327... | Fri Oct 26 01:28:58 PDT 2040 | 2
camerfirmachambersca [jdk] | X.509 | 3 | CN=Chambers of Commerce Root - 2008,O=AC Camerfirma... | Sat Jul 31 05:29:50 PDT 2038 | 11806822484801597146
camerfirmachamberscommerceca [jdk] | X.509 | 3 | CN=Chambers of Commerce Root,OU=http://www.chamber... | Wed Sep 30 09:13:44 PDT 2037 | 0
camerfirmachambersignca [jdk] | X.509 | 3 | CN=Global Chambersign Root - 2008,O=AC Camerfirma S.A... | Sat Jul 31 05:31:40 PDT 2038 | 14541511773111788494
cert_100_hellenic_academic_and_research_institutions_roo... | X.509 | 3 | CN=Hellenic Academic and Research Institutions RootCA 2... | Sat Jun 30 03:11:21 PDT 2040 | 0
cert_101_hellenic_academic_and_research_institutions_ec... | X.509 | 3 | CN=Hellenic Academic and Research Institutions ECC Roo... | Sat Jun 30 03:37:12 PDT 2040 | 0
cert_103_ac_raiz_fnmt_rcm103 | X.509 | 3 | OU=AC RAIZ FNMT-RCM,O=FNMT-RCM,C=ES | Mon Dec 31 16:00:00 PST 2029 | 485876308206448804701554682760554759
cert_108_tubitak_kamu_sm_ssl_kok_sertifikasi___surum_... | X.509 | 3 | CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1,OU... | Sun Oct 25 01:25:55 PDT 2043 | 1
cert_109_gdca_trustauth_r5_root109 | X.509 | 3 | CN=GDCA TrustAUTH R5 ROOT,O=GUANG DONG CE... | Mon Dec 31 07:59:59 PST 2040 | 9009899650740120186
cert_110_trustcor_rootcert_ca_1110 | X.509 | 3 | CN=TrustCor RootCert CA-1,OU=TrustCor Certificate Auth... | Mon Dec 31 09:23:16 PST 2029 | 15752444095811006489


System Admin
Take me to
EPS In : 0
EPS Out : 0
CPU : 1%
07:25
System
System Locale
System Reboot
Network
SMTP
Roles
License & Update
Process Status
SSH
SNMP
Logs
Audit Logs
Audit Forwarding
Storage
Remote File Systems
RAID Controller
Security
SSL Server Certificate
SSL Client Authentication
FIPS 140-2
Users/Groups
Authentication
Login Banner
User Management
Change Password
SSL Settings
Trusted Certificates
Certificate Revocation List
Upload Certificate
The certificate file needs to be in the PEM format.
Upload File
Browse...
Upload
Certificates in Repository
Certificate Name
Start date
Expiration Date
Delete

Questions?

Login Methods

- Local Password
- LDAP/LDAPS
- RADIUS

Questions?

Q&A