

# <u>Inhalt</u>

Der Einstieg	2
Das Problem	2
Ausgangsinformationen	2
Die Fehlersuche	3
Sichtung von Informationen	3
TroubleShooting-Methodik	6
Ausschlussverfahren: Deaktivierung aller Funktionen des Servers	6
Reaktivierung des SYSLOG-Services und des Eventlog-Forwardings	7
Reaktivierung des PRTG-Services	9
Detailsuche im Service PRIG	10
Der Auslöser	14
Die Lösung	19
Ein Workaround	19
neues Update – neuer Versuch	20
Zusammenfassung	24

# **Der Einstieg**

# Das Problem

Ich verwende in meiner Infrastruktur einen Windows Server 2019 für mein Monitoring. Dort laufen verschiedene Dienste, welche Informationen sammeln und aufbereiten. Bei Bedarf informiert mich das System per Mail oder mit Push-Notifications über Anomalien. Und natürlich kann ich die Informationen auch historisch analysieren, um beispielsweise Trends zu erkennen.

Heute habe ich festgestellt, dass es schon länger keine Warnmeldungen mehr vom Server gab. Das ist durchaus wünschenswert, aber in meinem Fall nicht normal. Denn den Server habe ich so eingestellt, dass er sich mindestens einmal am Tag per Mail meldet und eine Zusammenfassung sendet. Und diese blieb aus.

Das Problem war schnell gefunden: Der Server ist komplett ausgelastet. Im Taskmanager ist der verantwortliche Prozess deutlich erkennbar:

j⊠ Task-Manager Datei Optionen Ansicht			
Prozesse Leistung Benutzer Details Dier	nste		
^	Autoria	33%	94%
Anns (2)	natus	CPU	Arbeitss
> 🙀 Task-Manager		0%	15,7 MB
> 📧 Windows-Herunterfahrprogram		0%	1,1 MB
Hintergrundprozesse (23)			
> 📧 Antimalware Service Executable		0,3%	75,8 MB
> 📧 COM Surrogate		0%	2,1 MB
📧 Credential Guard & Key Guard		5,1%	1.210,4 MB
CTF-Ladeprogramm		0%	2,8 MB
> 🔟 Host für die Windows Shell-Obe	φ	0%	0 MB
📧 Hostprozess für Windows-Aufg		0%	1,8 MB

Hier möchte ich aufzeigen, wie man das Problem im Detail auf seine Ursache untersuchen kann.

# <u>Ausgangsinformationen</u>

Für jedes TroubleShooting sind zusätzliche Informationen erforderlich.

## System-Informationen

- Der Server heißt WS-MON und ist Mitglied meiner Active Directory Domain.
- Er läuft mit Windows Server 2019 und der Desktop Experience.
- Das System ist eine VM in einem Hyper-V-Server.

## Welche Dienste laufen auf dem Server?

- Der Server sammelt von allen anderen Servern die weitergeleiteten Ereignisse in einem zentralen Eventlog. Dafür nutze ich das Windows Eventlog Forwarding (WEF). Dieses habe ich über eine Gruppenrichtlinie "quell-initiiert" eingerichtet. Die anderen Server senden also die gefilterten Informationen an meinen WS-MON. Die Last sollte daher recht gering sein.
- Dazu ist ein KIWI-SYSLOG-Server installiert. Hier senden meine PFSense-Systeme (Firewall, IPS) ihre Logfiles her. Der SYSLOG-Server speichert die Daten in Textdateien.
- Auf WS-MON habe ich eine PRTG-Instanz installiert. Diese überwacht mit der freien Edition bis zu 100 Sensoren. In meinem Fall habe ich damit diverse Dienste und Komponenten meiner Infrastruktur agentfrei im Blick.
- Zudem laufen einige Scripte über geplante Aufgaben, mit denen ich Informationen sammle und analysiere.

## Was wurde zuvor verändert?

- Das System installiert Windows Updates vollautomatisch.
- PRTG darf sich ebenfalls automatisch Updates herunterladen und installieren.



• Die Belastungen auf dem System sollten sich eigentlich nicht verändern: Weder hat sich das Volumen der Eventlogs noch das der PFSense-Logfiles verändert.

#### Systemabsicherung

• Der Server wird durch verschiedene Gruppenrichtlinien für die Sicherheit gehärtet. Dazu gehört auch die Absicherung durch den Credential Guard.

#### Sonstiges

• Das System lief fehlerfrei seit der Installation vor einigen Monaten.

# **Die Fehlersuche**

## Sichtung von Informationen

Wie geht man nun an die Thematik heran? Zu den Ausgangsinformationen benötige ich Daten des aktuellen Systems. Glücklicherweise konnte ich mich auf dem Server noch anmelden. Alternativ wäre auch ein PowerShell-Remoting denkbar, denn diese Form der Verbindung benötigt nur sehr wenige Ressourcen.

Sollte eine Anmeldung nicht (mehr) möglich sein, dann könnte ein Neustart helfen. Ebenso könnte ich die ausgelastete Ressource (in meinem Fall der Arbeitsspeicher) nach oben skalieren. Aber auch ein Start im guten, alten abgesicherten Modus ist denkbar. Dann bleiben die ganzen Zusatzdienste aus – potentiell also auch die Problem-Komponente.

Einen Neustart hatte ich vor einigen Tagen schon durchgeführt. Das Problem konnte damit also nicht gelöst werden. Bei mir starten die Tools gerade noch, daher verzichte ich auf einen weiteren Neustart. Dieser könnte wertvolle Spuren verwischen. Ich erkenne deutlich den Prozess, der den Arbeitsspeicher bindet. LSAISO ist der "Isolated Local Security Authority"-Prozess. In diesem sind zur Laufzeit die "Geheimnisse" des Betriebssystems – also Passwörter, Hashes und dergleichen – gespeichert. Normalerweise übernimmt diese Aufgabe der LSASS-Prozess. Dieser stellt die eigentliche "Local Security Authority" dar. Durch den Credential Guard, der seit Windows Server 2016 und Windows 10 verwendet werden kann, werden die sensiblen Informationen noch einmal zusätzlich abgesichert.

Ich arbeite schon sehr lange mit dem Credential Guard. Er ist auch allen von meinen Servern und Clients aktiv. Doch diese Auslastung kenne ich so nicht:

🕎 Task-Manager	n Task-Manager												
Datei Optionen Ansich	ht												
Prozesse Leistung Ben	utzer De	etails Dienste											
Name	PID	Status	Benutzerna	CPU	Arbeitsspei	Arbeitsspei	Arbeitsspei	Seitenfehler	Ver	UAC-Virtualisi			
Lsalso.exe	740	Wird ausgeführt	SYSTEM	10	1.224.424 K	1.224.424 K	1.548 K	549.570	17	Nicht zugelass			
PRTG Server.exe	2828	Wird ausgeführt	SYSTEM	00	156.440 K	156.440 K	12.384 K	2.917.808	17	Nicht zugelass			
MsMpEng.exe	2916	Wird ausgeführt	SYSTEM	00	91.772 K	91.772 K	44.160 K	4.232.161	38	Nicht zugelass			
Isass.exe	748	Wird ausgeführt	SYSTEM	06	59.256 K	59.256 K	13.552 K	93.835	1	Nicht zugelass			
svchost.exe	1164	Wird ausgeführt	Netzwerkd	00	45.496 K	45.496 K	28.840 K	72.687	6	Nicht zugelass			
🔿 PRTG Probe.exe	2856	Wird ausgeführt	SYSTEM	00	44.676 K	44.676 K	20.756 K	44.605.365	63	Nicht zugelass			

Und wie zu erwarten war, begnügt sich der Prozess nicht mit dem physikalisch zugesicherten Speicher. Er lässt auch großzügig in die Auslagerungsdatei schreiben:

																í	
😰 Task-Manager																	-
Datei Optionen A	nsicht																
Prozesse Leistung	Benutzer D	Details Dienste															
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	UAC-Virtualisi		
Lsalso.exe	740	Wird ausgeführt	SYSTEM	06	01:02:11	986.976 K	985.484 K	985.484 K	1.492 K	2.202.908 K	25 K	104 K	556.199	83	Nicht zugelass		
PRTG Server.exe	2828	Wird ausgeführt	SYSTEM	00	00:26:52	168.572 K	156.188 K	156.188 K	12.384 K	234.348 K	266 K	117 K	2.957.534	26	Nicht zugelass		
MsMpEng.exe	2916	Wird ausgeführt	SYSTEM	00	00:15:56	130.716 K	84.336 K	84.336 K	46.380 K	160.596 K	630 K	69 K	4.305.815	6	Nicht zugelass		
Isass.exe	748	Wird ausgeführt	SYSTEM	04	00:34:44	72.732 K	59.180 K	59.180 K	13.552 K	61.824 K	226 K	33 K	94.236	0	Nicht zugelass		
mmc.exe	5144	Wird ausgeführt	stephan-T1	00	00:00:27	99.004 K	53.944 K	53.944 K	45.060 K	78.356 K	646 K	44 K	231.325	0	Nicht zugelass		
svchost.exe	1164	Wird ausgeführt	Netzwerkd	00	00:00:09	85.828 K	47.532 K	47.532 K	38.296 K	68.232 K	321 K	29 K	75.593	0	Nicht zugelass		
PRTG Probe.exe	2856	Wird ausgeführt	SYSTEM	00	06:00:31	65.440 K	44.684 K	44.684 K	20.756 K	64.088 K	316 K	51 K	45.168.286	0	Nicht zugelass		
Secure System	56	Wird ausgeführt	SYSTEM	00	00:00:00	30.248 K	30.248 K	30.248 K	0 K	176 K	8 K	0 K	754	0	Nicht zugelass		
svchost.exe	1156	Wird ausgeführt	SYSTEM	00	00:00:52	59.236 K	24.744 K	24.744 K	34.492 K	33.044 K	482 K	47 K	814.367	0	Nicht zugelass		
The second second	2764	Martine and a second state	OVETERA	00	00-00-14	27 176 V	20.020 K	20.020 K	16 DEC V	05 604 M	175 1/	22.14	221 646	0	KO ALE AND ALE A		

Dabei verdrängt er als systemkritischer Prozess andere Dienste und Anwendungen. In der Folge erhalte ich z.B. keine Informationen mehr vom Monitoring. Denn dieses hat selber keine Ressourcen mehr. Im Eventlog schreit der Server um



Hilfe. Leider wäre für die Weiterleitung dieses Hilferufs mein Monitoring zuständig gewesen, das auf dem betroffenen Server läuft ...



Im Anwendungs-Eventlog finde ich weitere Events, die der Auslastung vorangehen:



Anwendung Anzahl	von Ereignissen: 48.602			
Ebene		Datum und Uhrzei	t	Quelle
Fehler		21.12.2019 05:20:22	2	Perflib
Fehler		21.12.2019 05:20:19	9	Application Error
Fehler		21.12.2019 05:20:19	9	.NET Runtime
🕕 Fehler		21.12.2019 05:20:16	5	Application Error
🕕 Fehler		21.12.2019 05:20:16	5	.NET Runtime
🕕 Fehler		21.12.2019 05:19:59	9	.NET Runtime
🕕 Fehler		21.12.2019 05:19:45	5	Application Error
🕕 Fehler		21.12.2019 05:19:45	5	.NET Runtime
Fehler		21.12.2019 05:19:44	4	.NET Runtime
🕕 Fehler		21.12.2019 05:19:36	5	.NET Runtime
🕕 Fehler		21.12.2019 05:19:30	0	Application Error
Fehler		21.12.2019 05:19:30	0	.NET Runtime
Fehler		21.12.2019 05:19:28	3	Application Error
🕕 Fehler		21.12.2019 05:19:28	3	.NET Runtime
U Fehler		21.12.2019 05:19:21	1	.NET Runtime
U Fehler		21.12.2019 05:19:19	9	.NET Runtime
U Fehler		21.12.2019 05:19:16	5	.NET Runtime
<		21 12 2010 05 10 2	<u>(</u>	NUT D. 12
Ereignis 1023, Perflib Allgemein Details				
Windows kann die	erweiterbare Leistungsindik	kator-DLL "C:\Windows\Syst	em32\Perfctrs.dll" nicht laden (Wii	n32-Fehlercode Die Auslagerungsdatei ist zu klein, um diese
Protokollname:	Anwendung			
Quelle:	Perflib	Protokolliert:	21.12.2019 05:20:22	
Ereignis-ID:	1023	Aufgabenkategorie:	Keine	
Ebene:	Fehler	Schlüsselwörter:		
Benutzer:	Lokaler Dienst	Computer:	WS-MON.ws.its	

Und hier finde ich auch durch eine Filterung die Eventlogs, die mein PRTG-Monitoring kurz vor der Abschaltung schreibt:



Anwendung	g Anzahl von	Ereignissen: 48.602			
Gefilte	ert:Protokoll: Ap	plication; Quelle: PRTG Syster	m Anzahl der Ereigniss	e: 56	
Ebene			Datum und Uhrzei	t	Quelle
1 Information	tionen		31.12.2019 07:17:07	7	PRTG System
(i) Informa	tionen		31.12.2019 07:16:02	2	PRTG System
1 Information	tionen		27.12.2019 20:33:55	5	PRTG System
1 Information	tionen		27.12.2019 20:33:09	)	PRTG System
Information	tionen		27.12.2019 20:17:10	5	PRTG System
1 Information	tionen		27.12.2019 20:07:52	2	PRTG System
1 Information	tionen		27.12.2019 20:07:06	5	PRTG System
(i) Informa	tionen		23.12.2019 02:55:30	)	PRTG System
1 Information	tionen		23.12.2019 02:54:43	3	PRTG System
1 Informa	tionen		21.12.2019 08:17:52	2	PRTG System
1 Informa	tionen		18.12.2019 06:25:36	5	PRTG System
lnforma ≪	tionen		10 12 2010 06-24-50	1	DRTG System
Ereignis 0, F	PRIG System				
Allgemeir	n Details				
Core Se	erver will shut do	own now (running for 9 Min. 2	2 Sek. since 27.12.201	9 20:07:53) ID: -1000	
· ·					
Protokol	llname:	Anwendung			
Quelle:		PRTG System	Protokolliert:	27.12.2019 20:17:16	
Ereignis-	-ID:	0	Aufgabenkategorie:	Keine	
Ebene:		Informationen	Schlüsselwörter:	Klassisch	
Benutzer	r:	Nicht zutreffend	Computer:	WS-MON.ws.its	

# TroubleShooting-Methodik

Ich vergleiche gerne das betroffene System mit anderen, um nach Gemeinsamkeiten und Unterschieden zu suchen. Ist ein anderes System nicht betroffen und hat dieses beispielsweise die gleichen Updates installiert, dann liegt die Vermutung nahe, dass es nicht an den Updates liegt. Wobei das keinesfalls ausgeschlossen werden sollte. Vergleicht hier bitte immer artgleiche Server. Einen Domain Controller mit einem SQL-Server zu vergleichen ist sinnbefreit. In meiner Infrastruktur sind alle anderen Server im Normalbetrieb. Daher schließe ich vorsichtig das Betriebssystem aus.

Vielleicht hat sich die Belastung schrittweise erhöht und der Server benötigt einfach mehr Power? Dazu ist eine Trendanalyse sinnvoll. Leider ist diese in meinem Fall im PRTG-Server gespeichert. Und dieser läuft auf dem ausgelasteten Server. Die Information werde ich daher später analysieren. Aus der Erfahrung mit meinem Server kann ich aber bestätigen, dass die konfigurierte Menge an Arbeitsspeicher immer ausgereicht hat. Wäre diese langsam auf dieses Maß gestiegen, dann hätte PRTG einen Hilferuf abgesetzt. Die Belastung muss also recht schnell aufgebaut worden sein.

So fällt mein Verdacht auf die installierten Anwendungen und Dienste. Mit dem Ausschlussverfahren kann ich recht schnell die Ursache eingrenzen.

# Ausschlussverfahren: Deaktivierung aller Funktionen des Servers

Für den Beweis meiner These "Es ist eine installierte Anwendung bzw. ein Dienst" deaktiviere ich den PRTG, den SYSLOG-Server und das Eventlog-Forwarding. Anschließend starte ich den Server neu.

Nach der Anmeldung kontrolliere ich die Systemauslastung. Der LSAISO-Prozess nimmt sich den gewohnten Anteil am Arbeitsspeicher. Die Zahl verändert sich nur im KB-Bereich. Die Ursache ist also eine der installierten Komponenten!

🙀 Task-Manager															
Datei Optionen Ansich	nt														
Prozesse Leistung Benu	itzer D	etails Dienste													
~				_											
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	UAC-Virtualisi
📧 backgroundTaskHos	468	Angehalten	stephan-T1	00	00:00:00	15.372 K	0 K	56 K	15.316 K	4.308 K	235 K	14 K	4.566	0	Deaktiviert
CompatTelRunner.exe	3052	Wird ausgeführt	SYSTEM	00	00:00:00	44 K	40 K	40 K	4 K	936 K	39 K	5 K	1.255	0	Nicht zugelass
conhost.exe	3268	Wird ausgeführt	SYSTEM	00	00:00:00	1.272 K	492 K	492 K	780 K	6.636 K	140 K	9 K	3.820	0	Nicht zugelass
csrss.exe	3876	Wird ausgeführt	SYSTEM	00	00:00:00	5.308 K	1.392 K	1.392 K	3.916 K	2.360 K	172 K	12 K	1.739	0	Nicht zugelass
csrss.exe	504	Wird ausgeführt	SYSTEM	00	00:00:00	2.584 K	980 K	980 K	1.604 K	2.192 K	163 K	13 K	1.540	0	Nicht zugelass
csrss.exe	588	Wird ausgeführt	SYSTEM	00	00:00:00	1.252 K	324 K	324 K	928 K	1.696 K	112 K	9 K	1.369	0	Nicht zugelass
📝 ctfmon.exe	2684	Wird ausgeführt	stephan-T1	00	00:00:00	15.056 K	3.048 K	3.048 K	12.008 K	3.764 K	191 K	15 K	3.872	0	Deaktiviert
dwm.exe	4056	Wird ausgeführt	DWM-2	00	00:00:00	61.100 K	11.340 K	11.340 K	49.760 K	16.848 K	423 K	26 K	22.598	3	Deaktiviert
dwm.exe	1028	Wird ausgeführt	DWM-1	00	00:00:00	10.476 K	5.116 K	5.116 K	5.360 K	16.380 K	306 K	22 K	10.587	0	Deaktiviert
explorer.exe	4232	Wird ausgeführt	stephan-T1	00	00:00:02	53.336 K	11.200 K	11.200 K	42.136 K	23.068 K	804 K	58 K	23.559	2	Deaktiviert
fontdrvhost.exe	3996	Wird ausgeführt	UMFD-2	00	00:00:00	5.356 K	1.440 K	1.440 K	3.916 K	1.884 K	95 K	6 K	1.488	0	Deaktiviert
fontdrvhost.exe	936	Wird ausgeführt	UMFD-0	00	00:00:00	1.112 K	300 K	300 K	812 K	1.444 K	89 K	6 K	1.075	0	Deaktiviert
fontdrvhost.exe	928	Wird ausgeführt	UMFD-1	00	00:00:00	1.040 K	248 K	248 K	792 K	1.396 K	88 K	6 K	1.070	0	Deaktiviert
Leerlaufprozess	0	Wird ausgeführt	SYSTEM	98	00:05:32	8 K	8 K	8 K	0 K	56 K	0 K	0 K	8	0	
E LogonUl.exe	508	Wird ausgeführt	SYSTEM	00	00:00:00	43.316 K	7.928 K	7.928 K	35.388 K	10.812 K	501 K	26 K	13.886	0	Nicht zugelass
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:00	2.148 K	656 K	656 K	1.492 K	1.532 K	25 K	7 K	5.105	0	Nicht zugelass
Isass.exe	752	Wird ausgeführt	SYSTEM	00	00:00:00	13.860 K	5.108 K	5.108 K	8.752 K	7.540 K	131 K	31 K	5.688	0	Nicht zugelass

Für einen echten Beweis und für die Feindiagnose schalte ich nun eine Funktion nach der nächsten wieder ein. Wenn die Belastung mit dem Hochfahren eines Service wieder steigt, dann kenne ich den Verursacher.

# Reaktivierung des SYSLOG-Services und des Eventlog-Forwardings

Ich beginne mit dem SYSLOG-Service. Auch nach mehreren Minuten Betrieb verändert sich die Belastung des LSAISO-Prozesses nicht. Der KIWI-SYSLOG-Service ist es wohl nicht:

👰 Task-Manager														
Datei Optionen Ansic	ht													
Prozesse Leistung Ben	utzer D	etails Dienste												
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ve
∰WmiPrvSE.exe	3684	Wird ausgeführt	SYSTEM	00	00:00:00	5.228 K	1.112 K	1.112 K	4.116 K	2.380 K	76 K	9 K	3.357	
winlogon.exe	3920	Wird ausgeführt	SYSTEM	00	00:00:00	9.104 K	1.456 K	1.456 K	7.648 K	2.320 K	139 K	10 K	8.834	
csrss.exe	3876	Wird ausgeführt	SYSTEM	00	00:00:00	5.388 K	1.380 K	1.380 K	4.008 K	2.316 K	181 K	13 K	1.777	
csrss.exe	504	Wird ausgeführt	SYSTEM	00	00:00:00	2.160 K	916 K	916 K	1.244 K	2.196 K	160 K	12 K	1.725	
📧 svchost.exe	2700	Wird ausgeführt	SYSTEM	00	00:00:00	3.096 K	848 K	848 K	2.248 K	2.172 K	69 K	10 K	2.593	
💷 winlogon.exe	652	Wird ausgeführt	SYSTEM	00	00:00:00	1.520 K	592 K	592 K	928 K	2.048 K	129 K	10 K	3.545	
📧 svchost.exe	2064	Wird ausgeführt	Lokaler Di	00	00:00:00	6.020 K	1.140 K	1.140 K	4.880 K	2.020 K	95 K	12 K	2.528	
📧 svchost.exe	1316	Wird ausgeführt	Lokaler Di	00	00:00:00	3.572 K	772 K	772 K	2.800 K	1.976 K	78 K	12 K	2.309	
📧 RuntimeBroker.exe	4632	Wird ausgeführt	stephan-T1	00	00:00:00	7.780 K	1.180 K	1.180 K	6.600 K	1.776 K	117 K	8 K	2.097	
📧 svchost.exe	2548	Wird ausgeführt	SYSTEM	00	00:00:00	2.816 K	680 K	680 K	2.136 K	1.724 K	80 K	9 K	2.315	
VSSVC.exe	1816	Wird ausgeführt	SYSTEM	00	00:00:00	4.072 K	776 K	776 K	3.296 K	1.720 K	76 K	9 K	2.206	
csrss.exe	588	Wird ausgeführt	SYSTEM	00	00:00:00	628 K	280 K	280 K	348 K	1.644 K	110 K	9 K	1.436	
📧 svchost.exe	3148	Wird ausgeführt	Netzwerkd	00	00:00:00	2.784 K	596 K	596 K	2.188 K	1.592 K	57 K	12 K	2.286	
fontdrvhost.exe	936	Wird ausgeführt	UMFD-0	00	00:00:00	1.356 K	584 K	584 K	772 K	1.584 K	93 K	6 K	1.277	
📧 Registry	112	Wird ausgeführt	SYSTEM	00	00:00:00	62.236 K	1.268 K	1.268 K	60.968 K	1.500 K	178 K	7 K	25.121	
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:00	2.272 K	776 K	776 K	1.496 K	1.484 K	25 K	7 K	5.755	
📧 wininit.exe	580	Wird ausgeführt	SYSTEM	00	00:00:00	1.368 K	500 K	500 K	868 K	1.404 K	74 K	10 K	2.225	
fontdrvhost.exe	928	Wird ausgeführt	UMFD-1	00	00:00:00	652 K	244 K	244 K	408 K	1.368 K	88 K	5 K	1.101	
📧 smss.exe	388	Wird ausgeführt	SYSTEM	00	00:00:00	300 K	76 K	76 K	224 K	496 K	12 K	3 K	899	
📧 System	4	Wird ausgeführt	SYSTEM	00	00:00:07	136 K	20 K	20 K	116 K	192 K	0 K	0 K	1.580	
Secure System	56	Wird ausgeführt	SYSTEM	00	00:00:00	10.708 K	10.708 K	10.708 K	0 K	176 K	8 K	0 K	695	
💷 Leerlaufprozess	0	Wird ausgeführt	SYSTEM	99	00:28:09	8 K	8 K	8 K	0 K	56 K	0 K	0 K	8	
Systemunterbrechun	-	Wird ausgeführt	SVSTEM	00	00.00.00	0 K	0 K	0.K	0 K	0.K	0 K	0 K	0	
🔗 Weniger Details														

Jetzt aktiviere ich das Eventlog-Forwarding wieder. Die Aktion dauert etwas, da die anderen Server erst verzögert mit der Zustellung der Events beginnen. Daher warte ich einige Minuten ab und kontrolliere den Status der WEF-Clients:





Jetzt sind fast aller Server wieder online:

🛃 Ereignisanzeige								
Datei Aktion Ansicht ?								
🔿 🔁 📰 🛛 😨								
🚼 Ereignisanzeige (Lokal)	Abonnem	e <b>nts</b> 2 insg	esamt, 2	Aktiv.		_		
✓ → Benutzerdefinierte Ansichten	Name		Status	Typ	Quellcomp	Zielprotokoll	Beschreibung	
> Serverrollen	Defend	er	Aktiv	Ouellinitiiert	17	Weitergeleitete	beschiebung	
	Securit	/	Aktiv	Quellinitiiert	21	Weitergeleitete		
globales-AuditLog		,		Queinnerer		menergeneneren		
> 🖺 Windows-Protokolle								
> 💾 Anwendungs- und Dienstprotokolle								
Abonnements		📑 Laufzei	tstatus d	es Abonnement	ts - Security			×
		Abonnem	entstatu	s:				
		Aktiv - : K	ein weit	erer Status.				
		Quellcom	puter: 21	insgesamt, 14	Aktiv, 7 Inaktiv			
		Status	(	Computername				^
		🕢 Aktiv	1	NS-MON.ws.its				
		🕜 Aktiv	١	WS-MX1.ws.its				
		🛛 Aktiv	1	WS-MX2.ws.its				
		A Inakti	/ \	WS-NC1.ws.its				
		Aktiv		NS-NPS1.ws.its				
				NS-RA1.WS.Its				
		Aktiv		WS-RDS2.ws.its				
		Aktiv	Ň	WS-RDS3.ws.its				
		🕢 Aktiv	١	WS-WAC.ws.its				~
		<						>
		[WS-ATA.	ws.its] -	Aktiv - : Kein w	eiterer Status.			
								Schließen

Und der Problem-Prozess? Der begnügt sich mit seinen Ressourcen:

🙀 Task-Manager												
Datei Optionen Ansi	icht											
Prozesse Leistung Be	enutzer D	etails Dienste										
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg
Csrss.exe	3876	Wird ausgeführt	SYSTEM	00	00:00:01	5.480 K	1.408 K	1.408 K	4.072 K	2.364 K	177 K	13
svchost.exe	1080	Wird ausgeführt	Lokaler Di	00	00:00:00	7.140 K	1.392 K	1.392 K	5.748 K	2.312 K	85 K	9
csrss.exe	504	Wird ausgeführt	SYSTEM	00	00:00:00	2.176 K	920 K	920 K	1.256 K	2.196 K	159 K	12
svchost.exe	2700	Wird ausgeführt	SYSTEM	00	00:00:00	3.992 K	928 K	928 K	3.064 K	2.172 K	69 K	10
svchost.exe	2064	Wird ausgeführt	Lokaler Di	00	00:00:00	6.144 K	1.192 K	1.192 K	4.952 K	2.124 K	95 K	12
winlogon.exe	652	Wird ausgeführt	SYSTEM	00	00:00:00	1.736 K	612 K	612 K	1.124 K	2.048 K	129 K	10
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:01	2.752 K	1.208 K	1.208 K	1.544 K	1.940 K	25 K	13
📧 svchost.exe	1316	Wird ausgeführt	Lokaler Di	00	00:00:00	3.824 K	808 K	808 K	3.016 K	1.920 K	78 K	12
📧 svchost.exe	2548	Wird ausgeführt	SYSTEM	00	00:00:00	3.028 K	688 K	688 K	2.340 K	1.724 K	80 K	9
VSSVC.exe	1816	Wird ausgeführt	SYSTEM	00	00:00:00	4.100 K	780 K	780 K	3.320 K	1.720 K	76 K	9
csrss.exe	588	Wird ausgeführt	SYSTEM	00	00:00:00	636 K	288 K	288 K	348 K	1.644 K	110 K	9
📧 RuntimeBroker.exe	4632	Wird ausgeführt	stephan-T1	00	00:00:00	7.752 K	1.152 K	1.152 K	6.600 K	1.636 K	117 K	8
📧 svchost.exe	3148	Wird ausgeführt	Netzwerkd	00	00:00:00	2.816 K	600 K	600 K	2.216 K	1.592 K	57 K	12
fontdrvhost.exe	936	Wird ausgeführt	UMFD-0	00	00:00:00	1.432 K	632 K	632 K	800 K	1.584 K	93 K	6
📧 wininit.exe	580	Wird ausgeführt	SYSTEM	00	00:00:00	1.496 K	548 K	548 K	948 K	1.556 K	74 K	10
📧 fontdrvhost.exe	928	Wird ausgeführt	UMFD-1	00	00:00:00	652 K	244 K	244 K	408 K	1.368 K	88 K	5
📧 Registry	112	Wird ausgeführt	SYSTEM	00	00:00:00	60.252 K	272 K	272 K	59.980 K	500 K	178 K	7
smss.exe	388	Wird ausgeführt	SYSTEM	00	00:00:00	372 K	108 K	108 K	264 K	496 K	12 K	3
System	4	Wird ausgeführt	SYSTEM	00	00:00:09	136 K	20 K	20 K	116 K	192 K	0 K	0
Secure System	56	Wird ausgeführt	SYSTEM	00	00.00.00	10 708 K	10 708 K	10 708 K	0.K	176 K	8 K	0

Daher kann ich das Eventlog-Forwarding auch ausschließen.

## Reaktivierung des PRTG-Services

Es bleibt der Monitoring-Service PRTG über. Dieser besteht aus 2 Diensten. Zuerst starte ich den Core-Service. Dabei beobachte ich wieder die Auslastung des Prozesses LSAISO. Der Wert bleibt nahezu statisch.

]ݤ Task-Manager													
Datei Optionen Ansich	ıt												
Prozesse Leistung Benu	itzer De	tails Dienste											
Name	DID	Charles	Panutanana	CBU	CDU Z-à	Ashaitaata	Ashaitaanai	Ashaitaanai	Ashaitaanai	Zugesieher	Augustanas	Nichtause	Caitanfahlar
Indirie	FID	Status	Denutzenna	CFU	CF0-Zeit	AIDelissatz	Arbeitsspeim	Arbeitsspei	Arbeitsspei	zugesicher	Ausgelager	Nichtausg	Seitemener
dllhost.exe	736	Wird ausgeführt	SYSTEM	00	00:00:00	10.572 K	2.036 K	2.036 K	8.536 K	3.096 K	117 K	12 K	2.835
b msdtc.exe	3488	Wird ausgeführt	Netzwerkd	00	00:00:00	10.240 K	2.048 K	2.048 K	8.192 K	2.780 K	91 K	13 K	3.217
RuntimeBroker.exe	3112	Wird ausgeführt	stephan-T1	00	00:00:00	13.164 K	2.096 K	2.096 K	11.068 K	2.708 K	201 K	12 K	4.850
rdpclip.exe	972	Wird ausgeführt	stephan-T1	00	00:00:01	11.024 K	1.964 K	1.964 K	9.060 K	2.608 K	213 K	12 K	3.259
🔳 appidcertstorecheck	4072	Wird ausgeführt	Lokaler Di	00	00:00:00	8.528 K	2.052 K	2.052 K	6.476 K	2.584 K	93 K	11 K	2.542
svchost.exe	1080	Wird ausgeführt	Lokaler Di	00	00:00:00	7.156 K	1.412 K	1.412 K	5.744 K	2.400 K	85 K	9 K	3.571
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:02	3.168 K	1.624 K	1.624 K	1.544 K	2.380 K	25 K	18 K	36.880
winlogon.exe	3920	Wird ausgeführt	SYSTEM	00	00:00:00	9.360 K	1.504 K	1.504 K	7.856 K	2.332 K	139 K	11 K	13.536
csrss.exe	3876	Wird ausgeführt	SYSTEM	00	00:00:01	5.476 K	1.396 K	1.396 K	4.080 K	2.320 K	182 K	13 K	37.628
csrss.exe	504	Wird ausgeführt	SYSTEM	00	00:00:00	2.356 K	948 K	948 K	1.408 K	2.196 K	165 K	13 K	1.837
svchost.exe	2700	Wird ausgeführt	SYSTEM	00	00:00:00	3.988 K	904 K	904 K	3.084 K	2.068 K	69 K	10 K	3.109
💷 winlogon.exe	652	Wird ausgeführt	SYSTEM	00	00:00:00	1.748 K	612 K	612 K	1.136 K	2.048 K	129 K	10 K	3.616
📧 svchost.exe	2064	Wird ausgeführt	Lokaler Di	00	00:00:00	6.212 K	1.164 K	1.164 K	5.048 K	2.020 K	95 K	12 K	2.659
VSSVC.exe	1816	Wird ausgeführt	SYSTEM	00	00:00:00	7.336 K	1.156 K	1.156 K	6.180 K	1.980 K	90 K	10 K	3.143
📧 svchost.exe	1316	Wird ausgeführt	Lokaler Di	00	00:00:00	3.824 K	808 K	808 K	3.016 K	1.920 K	78 K	12 K	2.461
📧 svchost.exe	4192	Wird ausgeführt	SYSTEM	00	00:00:00	7.728 K	1.288 K	1.288 K	6.440 K	1.736 K	71 K	9 K	3.770
📧 svchost.exe	2548	Wird ausgeführt	SYSTEM	00	00:00:00	3.052 K	696 K	696 K	2.356 K	1.724 K	80 K	9 K	2.465
CSrSS.exe	588	Wird ausgeführt	SYSTEM	00	00:00:00	868 K	348 K	348 K	520 K	1.644 K	110 K	9 K	1.503

Zuletzt starte ich den zweiten Service "PRTG-Probes". Jetzt belegt der LSAISO-Prozess mehr Speicher. Ich merke mir dazu die aktuelle Uhrzeit:

🔁 Windows PowerShell								- 0	) ×						
Windows PowerShell Copyright (C) Microso	ft Corp	oration. Alle Rechte	vorbehalten.						^						
PS C:\Users\stephan-T	1> get-	date													
Mittwoch, 1. Januar 2	020 16:	16:17							- 1						
👰 Task-Manager															
Datei Optionen Ansic	ht														
Prozesse Leistung Ben	utzer De	etails Dienste													
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	ι
svchost.exe	1192	Wird ausgeführt	Lokaler Di	00	00:00:18	44.420 K	16.412 K	16.412 K	28.008 K	23.216 K	1.327 K	172 K	385.934	0	1
ShellExperienceHost	4456	Angehalten	stephan-T1	00	00:00:01	31.960 K	0 K	52 K	31.908 K	21.904 K	537 K	29 K	30.617	0	[
🙀 Taskmgr.exe	4708	Wird ausgeführt	stephan-T1	01	00:02:30	35.752 K	9.280 K	9.280 K	26.472 K	18.416 K	417 K	29 K	73.843	0	1
🚟 mmc.exe	3004	Wird ausgeführt	stephan-T1	00	00:00:02	47.164 K	9.220 K	9.220 K	37.944 K	17.716 K	532 K	37 K	31.165	0	٩
📧 svchost.exe	2540	Wird ausgeführt	SYSTEM	00	00:00:03	25.788 K	12.336 K	12.336 K	13.452 K	16.984 K	169 K	23 K	54.038	0	1
💷 dwm.exe	1028	Wird ausgeführt	DWM-1	00	00:00:00	10.964 K	5.476 K	5.476 K	5.488 K	16.304 K	292 K	20 K	11.194	0	C
📧 svchost.exe	1208	Wird ausgeführt	Lokaler Di	00	00:00:19	15.276 K	7.224 K	7.224 K	8.052 K	14.520 K	116 K	17 K	33.384	0	1
svchost.exe	776	Wird ausgeführt	Netzwerkd	00	00:01:05	21.540 K	8.456 K	8.456 K	13.084 K	12.708 K	233 K	42 K	27.866	0	1
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:15	12.660 K	11.068 K	11.068 K	1.592 K	12.036 K	25 K	19 K	42.555	0	1
svchost.exe	1352	Wird ausgeführt	SYSTEM	00	00:00:00	19.840 K	6.340 K	6.340 K	13.500 K	11.828 K	234 K	32 K	10.768	0	ľ

Nach 5 Minuten sind weitere 9 MB allokiert:

WS IT-Solutions

Windows PowerShell								— C	1 × 1						
									^						
PS C:\Users\stephan-	T1> get	-date													
Mittwoch, 1. Januar :	2020 16														
🔯 Task-Manager															
Datei Optionen Ansie	tt														
Prozesse Leistung Ber	nutzer D	Details Dienste													
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	1
ShellExperienceHost	. 4456	Angehalten	stephan-T1	00	00:00:01	31.972 K	0 K	64 K	31.908 K	21.904 K	537 K	29 K	30.620	0	ſ
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:29	21.544 K	19.952 K	19.952 K	1.592 K	21.212 K	25 K	20 K	44.790	0	1
Isass.exe	752	Wird ausgeführt	SYSTEM	00	00:00:15	27.992 K	18.072 K	18.072 K	9.920 K	20.776 K	165 K	32 K	15.890	0	I
- Tackmar ava	1700	Wird succeeführt	stanhan T1	01	00-03-45	05 016 V	0.244 %	0 244 1/	ע נדג אר	10 //76 V	117	20 1/	75 064	0	N
Windows PowerShell								- [	) ×						
									^						
PS C:\Users\stephan-	T1> get	-date													
Mittwoch, 1. Januar	2020 16	5:23:32							_						
									_						
PS C:\Users\stephan-	11>														-
Task-Manager															
Datei Optionen Ansi	cht														
Prozesse Leistung Be	nutzer	Details Dienste													
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	1
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:33	24.104 K	22.508 K	22.508 K	1.596 K	23.776 K	25 K	19 K	45.439	0	1
WmiPrvSE.exe	3828	Wird ausgeführt	SYSTEM	00	00:00:05	30.916 K	20.828 K	20.828 K	10.088 K	23.664 K	110 K	17 K	82.725	0	P

Das klingt nach nichts. Aber der Server soll 24/7 laufen. Und rein rechnerisch sind das unter der Annahme der linearen Steigerung 1,6MB je Minute. Das würde dann von jetzt bis 20:00 so aussehen:



In 24 Stunden wären mehr als 2GB Arbeitsspeicher belegt...

## Detailsuche im Service PRTG

Jetzt kenne ich die Komponenten, die das Problem verursachen: ein PRTG-Service auf einem Windows Server 2019 mit aktivem Credential Guard.

Ich benötige aber für die Fehlerbehebung weitere Informationen. Daher prüfe ich nun verschiedene Einstellungen im PRTG und beobachte deren Auswirkungen auf den LSAISO-Prozess.

Mein PRTG überwacht neben den Windows-Servern auch andere Geräte und Dienste. Ich habe einen Verdach, dass mein Problem durch die Windows Sensoren verursacht wird. Daher pausiere ich alle Sensoren, die für meine Windows Services gedacht sind:



<b>N</b> Startseite	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration			
Willkommen	pei PRTG											
Als Startseite	festlegen											
O Ü	bersicht	2 Tage	30 Tage	<b>365</b> Ta	age	Alarme	Proto	koll	≇ Verwaltung	0	Einstellungen	🜲 Trigge
✓ 19 I	67 (von 86)	S M L XL 🛞										Suche
	SFITS Gerät der Prob Serverz Netzwerk Server [[01.01 WS-HV4 F Upper V4 F	IE ID Systemzustand 100 % ✓ Systemzustand 100 % ✓ 16 Sen_ 2020 16:22:31 pausiert von 0 [[28.11.2019 10:21:13 p ID link 10 2 C: V 10 link 10 C: V 10 link 10	2ustand der Pr. 100% PRTG System Admin ausiert von PRTG Sy: 10 Diak IO 3 W: 15.28:00 (GMT+0)0 W 95-001	Sensor hinzufügen	bis 01.01.2020 16	<ul> <li>28:00 [GMT+0100</li> <li>01.2020 16:28:00 [</li> <li>11 W3-PFS1a</li> <li>11 W3-PFS1a</li> <li>11 Volume 10 V:</li> <li>11 W3-PFS1b</li> </ul>	) (GMT+0100) 1 WS-ATA 1 Volume IO W: 1 WS-RDS2	U WS-NPS1	WS-R051	1 Volume IO C:	Volume IO V:     Disk IO 2 V:	11 Disk 10 0 D:
	II NS-	DPM Volume IO C:	Volume IO D:	WS-PS2	Volume IO W:	Volume IO X:	WS-RDS2     Sensor	I RAM	Disk to o	DISKID TX:	Disk to 2 v:	In Disk to 3 C. W.
		T II 20 11 2010 10-21-21	DITC O		II. Developt his 01	01 2020 16-20-00	hinzufügen					
	I I I I I I I I I I I I I I I I I I I	TP Queue	DB-Jungbrunn.	. DB-Privat	DB-System	DB-WSITS	+ Sensor					
		<sup>3</sup> Pausiert bis 01.01.2020	16:28:00 [GMT+010	21			mitzurügen					
	" SM	rP Ueue	11 DB-Jungbrunn.	. II DB-Privat	II DB-System	II DB-WSITS	+ Sensor hinzufügen					
Ē	Image: WS-RDS3         Image: GS           Image: GS         Image: GS	[[09.08.2018 10:31:39]           ens           0         [[28.11.2019 10:21:31 p           1         Active Directo           0         [[11.06.2017 19:41:30 p           0         [[11.06.2017 19:41:30 p           0         [[11.06.2017 19:41:30 p           0         [[11.06.2017 19:41:30 p           0         [[10.08.2018 10:31:45 p	pausiert von PRTG Sys ausiert von PRTG Sys or 11 Active Director ausiert von PRTG Sys sr + Sensor hinzufügen ausiert von PRTG Sys	ystem Administrator stem Administrator - * Sensor hinzufügen stem Administrator stem Administrator	r ]]: Pausiert bis 01. ]]: Pausiert bis 01. ]]: Pausiert bis 01. ]]: Pausiert bis 01.	1.01.2020 16:28:00 01.2020 16:28:00 [ 01.2020 16:28:00 [ 01.2020 16:28:00 [ 01.2020 16:28:00 [	) [GMT+0100] [GMT+0100] [GMT+0100] [GMT+0100]					

Interessant: Seit der Pausierung stagniert der Hunger nach mehr Arbeitsspeicher vom LSAISO-Prozess wieder. Die Vermutung scheint richtig zu sein:

🔀 Windows PowerShell															
PS C:\Users\stephan-T	1> get-	date							^						
Mittwoch, 1. Januar 2	020 16:	25:25													
PS C:\Users\stephan-T	1>								_						
👰 Task-Manager															
Datei Optionen Ansic	ht														
Prozesse Leistung Ben	utzer De	tails Dienste													
															_
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	U١
Lsalso.exe	744	Wird ausgeführt	SYSTEM	00	00:00:33	24.100 K	22.504 K	22.504 K	1.596 K	23.772 K	25 K	20 K	45.445	0	N
WmiPrvSE.exe	3828	Wird ausgeführt	SYSTEM	00	00:00:05	31.048 K	20.960 K	20.960 K	10.088 K	23.732 K	110 K	17 K	82.766	0	N

Ich schalte einzelne Sensoren wieder ein. Mit jedem aktiven Windows-Sensor steigt der Arbeitsspeicherkonsum leicht an. Da habe ich mit meiner freien PRTG-Lizenz und max. 100 Sensoren durchaus Glück gehabt.

Vielleicht liegt es an der Kennung, die mein PRTG für den Remotezugriff verwendet? Diese ist ein Active Directory Benutzer, den ich als Service Account verwende. Ich konfiguriere einen anderen Benutzer-Account in den Sensoren. Durch die Vererbung der Einstellungen geht das recht schnell. Dann starte ich die Sensoren wieder. Leider nimmt sich der Credential Guard wieder mehr Speicher. Das Problem wird nicht durch den Service Account verursacht.

Vielleicht ist es gar nicht die PRTG-Konfiguration? Ich probiere die Deaktivierung des Device Guards. Dieser stellt auch den Credential Guard bereit. Die Aktivierung dieser Schutzkomponente übernimmt eine Gruppenrichtlinie:

#### GPO-Computer-Sicherheit-DeviceGuard

**F-Solutions** 

GPO-Computer-Sicherheit-DeviceGuard         Alle einbli         Computerkonfiguration (Aktiviert)         Aust         Richtlinien       Aust         Administrative Vorlagen       Aust         Richtlinien       Computer abgenden.         System/Device Guard       Aust         Richtlinie       Einstellung       Aust         Richtlinie       Finstellung       Aust         Richtlinie       Finstellung       Aust         Richtlinie       Finstellung       Aust         Richtlinie       Finstellung       Aust         Plattform-Sicherheit aktivieren       Aktivier         Plattform-Sicherheit aktivieren       Aktivier         Plattform-Sicherheit aktivieren       Aktivier         Vitualisierungsbasierter Schutz der Codeintegrit	reich Details Eir	nstellungen Delegierung Status			
Allgemein       Ent         Computerkonfiguration (Aktiviert)       Aust         Richtlinien       Aust         Administrative Vorlagen       Aust         Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.       Aust         System/Device Guard       Aust         Pichtlinie       Einstellung       Kommentar         Virtualisierungabasierte Sicherheit aktivieren       Aktiviert         Plattform-Sicherheitsstufe auswählen:       Sicherer Stat und DMA-Schutz       Virtualisierungabasierter Schutz der Codeintegrität:	GPO-Comp Daten ermittelt ar	m: 04.03.2020 07:45:32			Alle einblenden
Computerkonfiguration (Aktiviert)       Austivity         Richtlinien       Austivity         Administrative Vorlagen       Austivity         Richtlinien(ADMX-Dateien) wurden beim lokalen Computer abgerufen.       Austivity         System/Device Guard       Austivity         Richtlinie       Einstellung         Kommentar       Austivity         Virtualisierungsbasierte Sicherheit aktivieren       Aktiviert         Plattform-Sicherheitsatufe auswählen:       Sicherer Start und DMA-Schutz         Virtualisierungsbasierter Schutz der Codeintegrität:       Ohne Sperre aktiviert	Allgemein				Einblenden
Richtlinien         Administrative Vorlagen       Aust         Administrative Vorlagen       Aust         Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.       Aust         System/Device Guard       Aust         Fichtlinie       Einstellung       Kommentar         Virtualisierungsbasierte Sicherheit aktivieren       Aktiviert       Sicherer Stat und DMA-Schutz         Plattform-Sicherheitsstufe auswählen:       Sicherer Stat und DMA-Schutz       Ohne Sperre aktiviert	Computerkonfi	iguration (Aktiviert)			Aushlenden
Administrative Vorlagen     Administrative Vorlagen       Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.     Aust       System/Device Guard     Aust       Richtlinie     Einstellung       Virtualisierungsbasierte Sicherheit aktivieren     Aktiviert       Plattform-Sicherheitsstufe auswählen:     Sicherer Start und DMA-Schutz       Virtualisierungsbasierter Schutz der Codeintegrifät:     Ohne Sperre aktiviert	Richtlinien				Ausblenden
Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.         System/Device Guard         Fischtlinie       Einstellung       Kommentar         Virtualisierungsbasierte Sicherheit aktivieren       Aktiviert         Plattform-Sicherheitsstufe auswählen:       Sicherer Start und DMA-Schutz         Virtualisierungsbasierte Schutz der Codeintegrifät:       Ohne Sperre aktiviert	Administrat	tive Vorlagen			Ausblenden
Austo           Fichtlinie         Einstellung         Kommentar           Virtualisierungsbasierte Sicherhet aktivieren         Aktiviert         Plattform-Sicherhetsstufe auswählen:         Sicherer Start und DMA-Schutz           Virtualisierungsbasierter Schutz der Codeintegrität:         Ohne Sperre aktiviert         Ohne Sperre aktiviert	Ric	chtliniendefinitionen (ADMX-Dateien) wurden beim lok	alen Computer abgerufen.		Austrenden
Richtlinie     Einstellung     Kommentar       Vitualisierungsbasierte Sicherheit aktivieren     Aktiviert       Plattform-Sicherheitsstufe auswählen:     Sicherer Start und DMA-Schutz       Vitualisierungsbasierter Schutz der Codeintegrität:     Ohne Sperre aktiviert	System	n/Device Guard			Ausblenden
Virtualisierungsbasierte Sicherheit aktivieren         Aktiviert           Plattform-Sicherheitsstufe auswählen:         Sicherer Start und DMA-Schutz           Virtualisierungsbasierter Schutz der Codeintegrität:         Ohne Sperre aktiviert	Ri	ichtlinie	Einstellung	Kommentar	
Plattform-Sicherheitsstufe auswählen:     Sicherer Start und DMA-Schutz       Vitualisierungsbasierter Schutz der Codeintegrität:     Ohne Sperre aktiviert	Vir	rtualisierungsbasierte Sicherheit aktivieren	Aktiviert		
Virtualisierungsbasierter Schutz der Codeintegrität: Ohne Sperre aktiviert		Plattform-Sicherheitsstufe auswählen:		Sicherer Start und DMA-Schutz	
		Virtualisierungsbasierter Schutz der Codeintegrität	:	Ohne Sperre aktiviert	
UEFI-Speicherattributtabelle erforderlich Deaktiviert		UEFI-Speicherattributtabelle erforderlich		Deaktiviert	
Credential Guard-Konfiguration: Mit UEFI-Sperre aktiviert		Credential Guard-Konfiguration:		Mit UEFI-Sperre aktiviert	
Sichere Startkonfiguration:		Sichere Startkonfiguration:			
Benutzerkonfiguration (Deaktiviert)	Benutzerkonfig	guration (Deaktiviert)			Ausblenden

Ich nehme den Server aus deren Wirkungsbereich heraus, aktualisiere die Gruppenrichtlinienverarbeitung durch ein gpupdate und starte ihn neu. Da ich die Einstellung mit UEFI-Sperre aktiviert habe, wird das aber nicht genügen. Dazu ist etwas Hintergrundwissen hilfreich:

Der Device Guard soll das System auch vor Schadprogrammen schützen, die selber im Systemkontext laufen. Der LSAISO-Prozess kann im laufenden Betrieb nicht beendet werden. Zur Laufzeit ist das System also sicher. Aber ein Angreifer könnte die Einstellung für den Start des Device Guards verändern und das System neu starten. Dann wäre der Prozess nach dem Neustart aus und die Geheimnisse des Betriebssystems könnten abgegriffen werden.

Und genau hier greift die UEFI-Sperre. Die GPO erzeugt im UEFI eine Variable für den Device Guard Startmodus. Diese Variable wird auf ReadOnly konfiguriert. Sie kann also auch vom System selber nicht mehr zur Laufzeit verändert werden. Bei jedem Neustart prüft der LSASS-Prozess den Inhalt der Variable. Ist sie vorhanden und auf einen aktiven Device Guard konfiguriert, dann wird der LSAISO-Prozess gestartet – unabhängig davon, was die lokale Registry dazu sagt. Damit bleibt ein Device Guard auch nach dem Neustart aktiv – egal, welche Rechte ein Angreifer erbeutet hat.

Dieses hohe Schutzniveau behindert aber nicht nur Angreifer. Ich als Administrator muss jetzt zusätzliche Schritte unternehmen, um den Device Guard zu deaktivieren. Das einfache Entfernen der GPO wird nicht genügen, denn darin wird ja auch nur der Registry-Key verändert. Die UEFI-Variable kann das System ja selber nicht mehr verändern.

Für die Deaktivierung gibt es eine offizielle Anleitung von Microsoft. Dabei wird für den nächsten Neustart der UEFI-Boot um eine Sequenz erweitert. In dieser muss dann vor dem Start des Betriebssystems an der Konsole des Servers die Deaktivierung vom Device Guard explizit bestätigt werden. Man benötigt also einen physikalischen Zugang.

Für die Abschaltung stellt Microsoft eine efi-Datei bereit. Diese habe ich in der passenden x64-Variante direkt auf die C-Partition gespeichert. In meinem Server führe ich diese Zeilen in einer administrativen cmd aus:

```
mountvol X: /s
copy C:\LSAPPLConfig.efi X:\EFI\Microsoft\Boot\LSAPPLConfig.efi /Y
bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\LSAPPLConfig.efi"
bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions %1
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:
mountvol X: /d
```

```
shutdown -r -t 0
```

Der Server wird jetzt neugestartet. Auf der Konsole im Hyper-V stehen nun wenige Sekunden für die Abschaltung zur Verfügung:





Anschließend startet der Server wie gewohnt. Nur eben ohne den LSAISO-Prozess des Device Guards. Mit einem Blick ins msinfo kann ich die Abschaltung überprüfen:

	Verfügbarer physischer Speicher	275 MB
	Gesamter virtueller Speicher	7,34 GB
	Verfügbarer virtueller Speicher	5,97 GB
	Größe der Auslagerungsdatei	6,00 GB
	Auslagerungsdatei	C:\pagefile.sys
	Kernel-DMA-Schutz	Aus
	Virtualisierungsbasierte Sicherheit	Wird ausgeführt
	Virtualisierungsbasierte Sicherheit – erforderliche Sicherhe…	Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz
	Virtualisierungsbasierte Sicherheit – verfügbare Sicherheits	Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz, UEFI-Co
	Virtualisierungsbasierte Sicherheit – konfigurierte Dienste	Durch Hypervisor erzwungene Codeintegrität
	Virtualisierungsbasierte Sicherheit – ausgeführte Dienste	Durch Hypervisor erzwungene Codeintegrität
	Unterstützung der Geräteverschlüsselung	Nicht verfügbar
	Es wurde ein Hypervisor erkannt. Features, die für Hyper-V	
][		Suchen Suche schließen
(ategorie d	urchsuchen 🗌 Nur <u>K</u> ategorienamen durchsuchen	

Die PRTG-Services starten automatisch. Den LSAISO-Prozess gibt es weiter, denn dieser wird auch für das CodeIntegrity-Enforcement benötigt. Aber er begnügt sich mit wenig Arbeitsspeicher:

Registry 108 W														Dealerrier
le Registry 100 M	Vird ausgeführt	SYSTEM	00	00:00:00	62.088 K	1.076 K	1.076 K	61.012 K	1.328 K	178 K	7 K	25.213	0	Nicht zug
Lsalso.exe 740 V	Vird ausgeführt	SYSTEM	00	00:00:00	1.756 K	428 K	428 K	1.328 K	1.048 K	25 K	5 K	967	0	Nicht zug
📧 smss.exe 384 V	Vird ausgeführt	SYSTEM	00	00:00:00	848 K	196 K	196 K	652 K	504 K	12 K	3 K	889	0	Nicht zug
System 4 V	Vird ausgeführt	SYSTEM	00	00:00:07	152 K	20 K	20 K	132 K	192 K	0 K	0 K	1.555	0	
E Secure System 56 V	Vird ausgeführt	SYSTEM	00	00:00:00	10.732 K	10.732 K	10.732 K	0 K	176 K	8 K	0 K	700	0	Nicht zug
Eleerlaufprozess 0 V	Vird ausgeführt	SYSTEM	72	00:14:11	8 K	8 K	8 K	0 K	56 K	0 K	0 K	8	0	
	C 1 (C) 1	OVETERA	00	00.00.00	0.17	0.17	0.17	0.17	0.17	0.17	0.17	•	0	

Für einen echten Beweis verschiebe ich den Server wieder in den Einflussbereich der DeviceGuard GPO. Ein gpupdate und einen Neustart ist er wieder online. Msinfo zeigt die Präsens:

Auslagerungsdatei	C:\pagefile.sys
Kernel-DMA-Schutz	Aus
Virtualisierungsbasierte Sie	herh Wird ausgeführt
Virtualisierungsbasierte Sie	herh Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz
Virtualisierungsbasierte Sie	herh Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz, UEFI-Co
Virtualisierungsbasierte Sie	herh Credential Guard, Durch Hypervisor erzwungene Codeintegrität
Virtualisierungsbasierte Sie	herh Credential Guard, Durch Hypervisor erzwungene Codeintegrität
Unterstützung der Gerätev	ersc Nicht verfügbar
Es wurde ein Hypervisor e	kan
	Suchen Suche schließen
ählte Kategorie durchsuchen 🛛 Nur <u>K</u> ated	orienamen durchsuchen

Und der Taskmanager zeigt den LSAISO-Prozess mit seinem Memory Leak...

🙀 Task-Manager															
Datei Optionen Ar	nsicht														
Prozesse Leistung	Benutzer D	etails Dienste													
Name	PID	Status	Benutzerna	CPU	CPU-Zeit	Arbeitssatz	Arbeitsspei	Arbeitsspei	Arbeitsspei	Zugesicher	Ausgelager	Nichtausg	Seitenfehler	Ver	UAC
🖶 spoolsv.exe	2516	Wird ausgeführt	SYSTEM	00	00:00:00	15.824 K	4.496 K	4.496 K	11.328 K	5.868 K	215 K	23 K	4.523	0	Nich
svchost.exe	4636	Wird ausgeführt	stephan-T1	00	00:00:00	26.252 K	4.672 K	4.672 K	21.580 K	5.840 K	259 K	18 K	7.435	0	Deal
dllhost.exe	468	Wird ausgeführt	stephan-T1	00	00:00:00	12.480 K	2.372 K	2.372 K	10.108 K	5.424 K	144 K	22 K	5.403	0	Deal
sihost.exe	4604	Wird ausgeführt	stephan-T1	00	00:00:00	23.320 K	4.108 K	4.108 K	19.212 K	5.256 K	246 K	17 K	6.474	0	Deal
svchost.exe	84	Wird ausgeführt	Netzwerkd	00	00:00:01	12.040 K	3.912 K	3.912 K	8.128 K	4.996 K	103 K	27 K	3.782	2	Nich
NisSrv.exe	3804	Wird ausgeführt	Lokaler Di	00	00:00:00	10.412 K	2.784 K	2.784 K	7.628 K	4.872 K	137 K	12 K	3.448	22	Nich
Lsalso.exe	740	Wird ausgeführt	SYSTEM	08	00:00:04	7.344 K	4.148 K	4.148 K	3.196 K	4.748 K	25 K	7 K	18.898	18	Nich
services.exe	724	Wird ausgeführt	SYSTEM	00	00:00:00	8.640 K	3.820 K	3.820 K	4.820 K	4.448 K	131 K	11 K	2.804	0	Nich

Der Beweis ist erbracht: Der Credential Guard des Device Guards kann nicht mit dem PRTG Probe Service umgehen, wenn im PRTG Windows Server remote überwacht werden.

## Der Auslöser

Die Ursache für das direkte Problem ist identifiziert. Aber der Auslöser ist noch nicht bekannt. Den Server betreibe ich seit Monaten problemfrei.

Für die Suche nach dem Auslöser gibt es verschiedene Strategien, die mit unterschiedlichen Fragen verfolgt werden:

- Wann trat das Problem das erste Mal auf? Ggf. wurden zu dieser Zeit Konfigurationen oder Komponenten angepasst...
- Gibt es ein Muster im Problemverlauf? Vielleicht tritt ein Problem immer zu einer bestimmten Zeit auf? Eventuell kann aber auch ein zeitunabhängiger Trigger identifiziert werden, z.B. eine Anmeldung...

Die erste Frage ist meist einfacher zu beantworten. Interessanter Weise hilft mir hier mein jetzt wieder funktionales Monitoring. Der PRTG-Service überwacht sich selber. Und die Daten werden für Trendanalysen und Blicke in die Vergangenheit gespeichert. Also rufe ich den passenden Sensor auf:





Der Text im Bild ist recht klein, aber man erkennt sehr gut den Ausfallzeitraum. Auch kann man meinen Versuch "Reboot tut gut" nach der ersten Downtime erkennen. Und dass dieser nicht sehr lange hergehalten hat. Ebenso erkennt man, wie lange mein TroubleShooting gedauert hat. Und sehr wichtig ist auch die Aussage: Vorher gab es das Problem nicht – bis auf wenige Klicke ist der Statusgraph bei 100%.

Ich zoome etwas weiter rein:



Jetzt erkennt man deutlich den 18.12.2019 als Startzeitpunkt. Und vielleicht erklären sich jetzt auch die langen Unterbrechungen ohne meine Anteilnahme.

Mit dieser Information geht es weiter im Eventlog. Was passierte in der Früh des 18.12.? Es gab einen Neustart:



System Anzahl von Ereig	gnissen: 59.378 (!) Neue Ereigni	sse sind verfügbar				
Ebene	Datum und Uhrzeit		Quelle	Ereignis-ID	Aufgabenkategorie	
(i) Informationen	18.12.2019 06:24:39		FilterManager	6	Keine	
(i) Informationen	18.12.2019 06:24:39		Ntfs (Microsoft-Windo	98	Keine	
(i) Informationen	18.12.2019 06:24:39		FilterManager	6	Keine	
(i) Informationen	18.12.2019 06:24:39		FilterManager	6	Keine	
(i) Informationen	18.12.2019 06:24:39		Kernel-General	20	(6)	
<ol> <li>Informationen</li> </ol>	18.12.2019 06:24:39		IsolatedUserMode	3	Keine	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	30	(21)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	32	(58)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	18	(57)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	27	(33)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	25	(32)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	20	(31)	
(i) Informationen	18.12.2019 06:24:39		Kernel-Boot	153	(62)	
Informationen	18.12.2019 06:24:39		Kernel-General	12	(1)	
(i) Informationen	18.12.2019 06:24:33		Kernel-General	13	(2)	
(i) Informationen	18.12.2019 06:24:33		Kernel-Power	109	(103)	
U Fehler	18.12.2019 06:24:32		DistributedCOM	10028	Keine	
🕒 Fehler	18.12.2019 06:24:32		DistributedCOM	10028	Keine	
Ereignis 12, Kernel-Genera						
Allgemein Details						
Das Betriebssystem wu	irde zur Systemzeit 2019-12-18	105:24:58.5000000002	gestartet.			
Protokollaamo	Surtem					
Protokoliname:	System					
Quelle:	Kernel-General	Protokolliert:	18.12.2019 06:24:39			
Ereignis-ID:	12	Aufgabenkategorie:	(1)			
Ebene:	Informationen	Schlüsselwörter:	(128)			
Benutzer:	SYSTEM	Computer:	WS-MON.ws.its			
Vorgangscode:	Info					
Weitere Informationen:	<u>Onlinehilfe</u>					

Aber warum hat sich der Server neugestartet? So viele Optionen gibt es da nicht. Ich war es nicht. Andere Administratoren gibt es bei mir noch nicht. Also war es der Server selber. Und das macht er nur bei Windows Updates. Die passenden Events finde ich ein paar Einträge weiter unten:



-

Ereignisanzeige					
Datei Aktion Ansicht ?					
🗢 🔿 📶 🚺 🖬					
Ereignisanzeige (Lokal)	System Anzahl von Ereig	nissen: 59.721 (!) Neue Ereig	nisse sind verfügbar		
Vindows-Protokolle	Ebene	Datum und Uhrzeit	t	Quelle	
Anwendung	<ol> <li>Informationen</li> </ol>	18.12.2019 03:00:38	3	Service Control Manager	
Sicherheit	<ol> <li>Informationen</li> </ol>	18.12.2019 03:00:07	7	Service Control Manager	
Installation	<ol> <li>Informationen</li> </ol>	18.12.2019 03:00:07	7	Kernel-General	
💽 System	Informationen	18.12.2019 03:00:06	õ	WindowsUpdateClient	
Weitergeleitete Ereignisse	<ol> <li>Informationen</li> </ol>	18.12.2019 03:00:03	3	Service Control Manager	
Anwendungs- und Dienstpro	Essination 42 Windowed Indet	teClient			
Abonnements	Ereignis 45, WindowsOpda	techent			
	Allgemein Details				
	Installation gestartet: W (KB4533094)	/indows hat mit der Installat	ion des folgenden Upda	tes begonnen: 2019-12 Kumulativ	es Update f
	(101555554)				
	Protokollname:	System			
	Quelle:	WindowsUpdateClient	Protokolliert:	18.12.2019 03:00:06	
	Ereignis-ID:	43	Aufgabenkategorie:	Windows Update-Agent	
	Ebene:	Informationen	Schlüsselwörter:	Gestartet, Installation	
	Reputzer	SVSTEM	Computer	WS-MON we ite	
	Denutzei.	JIJI LIVI	computer	W0-W0W0W0W0	
	Vorgangscode:	Installation			
	Weitere Informationen:	Onlinehilfe			
< >					

Und nach dem Neustart wurden die Updates als installiert markiert:

🛃 Ereignisanzeige					
Datei Aktion Ansicht ?					
🗢 🄿 🙋 💼 🚺					
Ereignisanzeige (Lokal)	Installation Anzahl von E	reignissen: 96			
> Benutzerdefinierte Ansichten Vindows-Protokolle	Ebene	Datu	m und Uhrzeit		Quelle
Anwendung	(i) Informationen	21.01		Servicing	
Sicherheit	(i) Informationen	21.01	.2020 03:00:09		Servicing
Installation	(i) Informationen	23.12	2.2019 05:00:14		Servicing
🛃 System	Informationen	18.12	2.2019 06:25:00		Servicing
Weitergeleitete Ereignisse	(i) Informationen	18.12	2.2019 03:12:04		Servicing
> Anwendungs- und Dienstpro	Informationen	18 12	2019.03-00-56		Servicing
Abonnements	Ereignis 2, Servicing				
	Der Status des Pakets K	84530715 wurde erfolg	reich in "Installiert" geändert.		
	Protokollname:	Installation			
	Quelle:	Servicing	Protokolliert:	18.12.2019 06:25:00	)
	Ereignis-ID:	2	Aufgabenkategorie:	(1)	
	Ebene:	Informationen	Schlüsselwörter:		
	Benutzer:	SYSTEM	Computer:	WS-MON.ws.its	
	Vorgangscode:	Info			
	Weitere Informationen:	Onlinehilfe			

Ein Blick in den Update-Verlauf zeigt die Installation mit dem Datum an (Das Bild habe ich später neu erstellen müssen):

÷	Einstellungen	-	×
<u>ش</u>	Updateverlauf anzeigen		
Upda	ates deinstallieren		
Wied	lerherstellungsoptionen		
Upc	dateverlauf		
$\sim$	Qualitätsupdates (22)		
	Update für Windows Defender Antivirus-Antischadsoftwareplattform – KB4052623 (Version 4.18.2001.10)		
	Erfolgreich installiert am 02.03.2020		
	2020-02 Sicherheitsupdate für Adobe Flash Player für Windows Server 2019 für x64-basierte Systeme (KB4537759)		
	Erfolgreich installiert am 25.02.2020		
	2020-02 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4532691)		
	Erfolgreich installiert am 25.02.2020		
	2020-01 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4535669)		
	Erfolgreich installiert am 04.02.2020		
	2020-01 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4535101)		
	Erfolgreich installiert am 28.01.2020		
	2020-01 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4534273)		
	Erfolgreich installiert am 21.01.2020		
	2019-12 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4530715)		
	Erfolgreich installiert am 18.12.2019		
	2019-12 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4533094)		
	Erfolgreich installiert am 18.12.2019		
1			

Es muss also in mit einem dieser beiden Updates eine Änderung vorgenommen worden sein. Im Update KB4530715 (<u>https://support.microsoft.com/en-us/help/4530715/windows-10-update-kb4530715</u>) sieht es in der Übersicht schon recht treffend aus. Der Device Guard ist schließlich ein Sicherheitsfeature:

# Improvements and fixes

**IT-Solutions** 

This security update includes quality improvements. Key changes include:

- Addresses an issue with diagnostic data processing when a device has the Diagnostic data setting enabled and set to Basic.
- Addresses an issue in which the Microsoft Store might fail to open on Windows on Arm.
- Security updates to Windows Virtualization, Windows Kernel, Windows Peripherals, the Microsoft Scripting Engine, and Windows Server.

If you installed earlier updates, only the new fixes contained in this package will be downloaded and installed on your device.

For more information about the resolved security vulnerabilities, please refer to the Security Update Guide.

# Ich folge dem Link "Security Update Guide" (<u>https://portal.msrc.microsoft.com/en-us/security-guidance</u>) und finde die zum KB dazugehörige CVE-Nummer heraus

12/10/2019	Windows 10 Version 1809 for ARM64-based Systems	4530715	Security Update	CVE-2019-1469
12/10/2019	Windows Server 2019	4530715	Security Update	CVE-2019-1469
12/10/2019	Windows Server 2019 (Server Core installation)	4530715	Security Update	CVE-2019-1469
12/10/2019	Windows 10 Version 1709 for 32-bit Systems	4530714	Security Update	CVE-2019-1469

Viel interessanter ist aber der Link zu den Dateien, die vom Update geändert wurden. Diesen finde ich auf der Hauptseite des KBs.

Mattps://support.microsoft.com/en-us/help/4530715/windows-10-update-kb4530715									
Windows Server Update Services (WSUS)	Yes Product: Windows 10 Classification: Security Updates								

File information

**T-Solutions** 

For a list of the files that are provided in this update, download the file information for cumulative update 4530715.

Die Datei ist wie üblich schlecht strukturiert, aber ich finde die Lsaiso.exe gelistet.

<del>ت</del> 🖬	<b>□ 5 · ♂ ·</b> ⊽ 4530715.csv - Excel															
Datei	Start	Einfügen	Seitenlayout	FormeIn	Daten	Überprüfe	n Ansicht Hilfe	e ♀ ₩as m	nöchte	n Sie tun?						
Aus Text/CSV Calletzt verwendete Quellen Daten abrufen - Aus Tabelle/Bereich aktua						Alle	☐ Abfragen und Eigenschafter en - Q Verknüpfunge	l Verbindungen n en bearbeiten	A.	Sortieren	Filtern	✓ Löschen ✓ Erneut ar ✓ Erweitert	nwenden	Text in Spalten		W
	C	Daten abrufen	und transformiere	n			Abfragen und Verbindu	ngen		S	ortieren un	d Filtern		Datentool		
A209919	-	$\cdot$ ×	$\checkmark f_x$													
			A				В	С		D	)	E	Ξ	F		
1	File r	name				Л	File version -	File size	-	Date	Ŧ	Time	*	Platform	•	- 5
32246	Lsais	o.exe					Not applicab	l	5,5	4-Dec-1	19		03:09	Not appli	cable	•
32247	Lsais	o.exe					Not applicab	l 5,	608	4-Dec-1	19		03:09	Not appli	cable	;
209918																
209919																

# Die Lösung

## **Ein Workaround**

Ich sehe 2 ordentliche Möglichkeiten für die Lösung meiner Problematik:

- Microsoft korrigiert den Fehler im Credential Guard mit einem späteren Update.
- PRTG passt seine Anmeldeprozesse an bzw. gibt Hinweise zum Arbeiten in Umgebungen mit aktivem Credential Guard.

Beide Lösungen werden Zeit benötigen. Diese hat mein Server aber nicht. Daher werde ich bis zur finalen Lösung den Device Guard auf diesem einen Server deaktivieren. Dafür erstelle ich eine separate GPO mit der Einstellung und wende diese gefiltert auf meinen PRTG-Server an. Hier sieht man die GPO mit der Device Guard Deaktivierung. Sie wird in der Rangfolge vor der Richtlinie mit der Aktivierung angewendet. Damit "gewinnt" ihre Einstellung:



#### Server

Verknüpfte Gruppenrichtlinienobjekte Gruppenrichtlinienvererbung Delegierung

Die Liste enthält keine mit Standorten verknüpften Gruppenrichtlinienobjekte. Weitere Informationen erhalten Sie in der Hilfe.

Rangfolg	e Gruppenrichtlinienobjekt	Speicherort	Objektstatus	WMI-Filter
🗊 1	GPO-Computer-WSUS-Manuell	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
1 2	GPO-Computer-Sicherheit-Audit	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
<b>3</b>	GPO-Computer-Sicherheit-Audit-WEF	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
<b>4</b>	GPO-Computer-Sicherheit-Applocker	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
5	GPO-Computer-Sicherheit-DeviceGuard-aus	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
<b>6</b>	GPO-Computer-Sicherheit-DeviceGuard	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
7	GPO-Computer-Sicherheit-LAPS-Server	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
8	GPO-Computer-Sicherheit-LSAProtection	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
<b>F</b> 9	GPO-Computer-Sicherheit-Cipher-TLS	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🗊 10	GPO-Computer-Sicherheit-Firewall	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🗊 11	GPO-Computer-Sicherheit-Defender	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
12	GPO-Computer-Sicherheit-Basics	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🗊 13	GPO-Computer-Sicherheit-PowerShellWinRM	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🛒 14	GPO-Computer-Sicherheit-Netzwerk	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🔊 15	GPO-Computer-Sicherheit-Zertifikate	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🗊 16	GPO-Computer-Sicherheit-Firefox	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🛒 17	GPO-Computer-Sicherheit-IExplore	Server	Benutzerkonfigurationseinstellungen deaktiviert	Keine
🔊 18	GPO-Server-Win2016	Server	Benutzerkonfigurationseinstellungen deaktiviert	Windows-Server-2016
🗊 19	GPO-Server-Win2019-Datenschutz	Server	Benutzerkonfigurationseinstellungen deaktiviert	Windows-Server-2019
7 20	GPO-Server-Win2019-Konfiguration	Server	Benutzerkonfigurationseinstellungen deaktiviert	Windows-Server-2019
1 21	GPO-Server-Win2019-Sicherheit	Server	Benutzerkonfigurationseinstellungen deaktiviert	Windows-Server-2019
22	Default Domain Policy	ws.its	Benutzerkonfigurationseinstellungen deaktiviert	Keine

Damit aber nur der Monitor-Server editiert wird, verwende ich einen Sicherheitsfilter:

Dereicht	Details	Einstellungen	Delegierung	Status			
/erknū	pfunger	1					
ür diese	es Verzeio	chnis anzeigen:	ws.its				
)ie folge	enden Sta	ndorte, Domäne	n und Organisa	ationseinheiten sind	d mit dem Objekt verknüpft:		
Pfad		^		Erzwungen	Verknüpfung aktiviert	Pfad	
💼 Ser	ver			Nein	Ja	ws.its/WS/Server	
<b>ichert</b> lie Einst iruppen Name	n <b>eitsfilte</b> tellungen 1, Benutze	<b>rung</b> dieses Gruppen er und Computer	richtlinienobjek	ts gelten nur für die	folgenden		
<b>Sichert</b> )ie Einst iruppen Name	neitsfilte tellungen b, Benutze G-MON\$ ()	rung dieses Gruppen er und Computer WS\WS-MON <b>\$</b> )	richtlinienobjek	ts gelten nur für die	folgenden		
ichert Vie Einst iruppen Name MS	neitsfilte tellungen b, Benutze G-MON\$ ( zufügen	rung dieses Gruppen er und Computer WS\WS-MON\$)	richtlinienobjek	ts gelten nur für die Eigenschafter	folgenden		
ichert Die Einst Diruppen Name Mame WS	neitsfilte tellungen , Benutze S-MONS ( S-MONS (	rung dieses Gruppen er und Computer WS\WS-MON\$) . Er	tfemen	ts gelten nur für die Eigenschafter	folgenden		
Sichert Die Einst iruppen Name WS Hin VMI-Fi	neitsfilte tellungen a, Benutze S-MONS ( zufügen	rung dieses Gruppen er und Computer WS\WS-MON\$) . Er	tfemen	ts gelten nur für die Eigenschafter	folgenden		

Natürlich muss ich dafür die Prozedur mit dem UEFI-Unlock erneut ausführen.

## <u>neues Update – neuer Versuch</u>

Es sind nun einige Wochen vergangen. Der Server läuft ohne den Credential Guard wieder stabil. Zwischenzeitlich hat mein Server das Update vom Februar (2020-02) installiert:

← Einstellungen

# ☆ Updateverlauf anzeigen

Updates deinstallieren

Wiederherstellungsoptionen

# Updateverlauf

✓ Qualitätsupdates (22)

Update für Windows Defender Antivirus-Antischadsoftwareplattform – KB4052623 (Version 4.18.2001.10) Erfolgreich installiert am 02.03.2020

2020-02 Sicherheitsupdate für Adobe Flash Player für Windows Server 2019 für x64-basierte Systeme (KB4537759) Erfolgreich installiert am 25.02.2020

2020-02 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4532691)

Erfolgreich installiert am 25.02.2020

Ein Blick ins Dateisystem verrät, dass eine LSA-DLL modifiziert wurde. Das könnte eine neue Chance für die Reaktivierung des Device Guards sein:

> Dieser PC > System (C:) > Windows > System32 V 🖑							
ng	^	Name	Änderungsdatum	Тур	Größe		
n		LogonController.dll	16.10.2019 03:07	Anwendungserwe	776 KB		
ckages		LogonUl.exe	15.09.2018 09:12	Anwendung	14 KB		
		lpk.dll	15.09.2018 09:12	Anwendungserwe	3 KB		
		📑 Ipkinstall.exe	12.03.2019 07:31	Anwendung	41 KB		
		🐏 lpksetup.exe	15.09.2018 09:12	Anwendung	722 KB		
		Ipksetupproxyserv.dll	15.09.2018 09:12	Anwendungserwe	10 KB		
		Ipremove.exe	15.09.2018 09:12	Anwendung	57 KB		
		Lsalso.exe	11.10.2019 03:07	Anwendung	272 KB		
files		Sasrv.dll	25.02.2020 03:05	Anwendungserwe	1.636 KB		
te		Isass.exe	15.09.2018 09:12	Anwendung	57 KB		
		LSCSHostPolicy.dll	21.01.2020 03:04	Anwendungserwe	62 KB		
		lsm dll	11 10 2019 03:07	Anwendungsenwe	643 KB		

Ich deaktiviere die GPO, mit der ich für diesen einen Server die Abschaltung vorgenommen habe. Damit "gewinnt" wieder die andere Richtlinie und der Credential Guard sollte reaktiviert werden:

# WS IT-Solutions WSHowTo – Device Guard vs. PRTG 2020-01-01 Windows Server TroubleShooting

and a large		er-sicherne	eit-Device	Guard-aus			
reich	Details	Einstellungen	Delegierung	Status			
erknū	pfungen	1					
ir diese	es Verzeic	hnis anzeigen:	ws.its				
ie folge	enden Sta	ndorte, Domäne	n und Organis	ationseinheiten sind r	mit dem Objekt verknüpft:		
Pfad		^		Erzwungen	Verknüpfung aktiviert	Pfad	
Ser	ver			Nein	Nein	ws.its/WS/Server	
ichert	neitsfilte	100					
<b>ichert</b> )ie Einst iruppen	<b>neitsfilte</b> tellungen , Benutze	r <b>ung</b> dieses Gruppenr r und Computer:	ichtlinienobjek	ts gelten nur für die fr	olgenden		
<b>ichert</b> lie Einst iruppen Name	<b>neitsfilte</b> tellungen , Benutze	r <b>ung</b> dieses Gruppenr r und Computer:	ichtlinienobjek	ts gelten nur für die f	olgenden		
<b>iichert</b> )ie Einst iruppen Name	neitsfilter tellungen , Benutze	rung dieses Gruppenr r und Computer: WS\WS-MON\$)	ichtlinienobjek	ts gelten nur für die f	olgenden		
<b>iichert</b> )ie Einst iruppen Name <b>Name</b>	neitsfilter tellungen , Benutze G-MON\$ (N	rung dieses Gruppenr r und Computer: WS\WS-MON\$)	ichtlinienobjek	ts gelten nur für die fo	olgenden		

Ich beschleunige den Vorgang durch ein gpupdate auf meinem Monitor-Server. Mit msinfo sehe ich bereits die Einstellung. Diese greift aber erst nach einem Neustart:

Administrato Windows Powers Copyright (C)	r:Windows PowerShell hell Microsoft Corporation. Alle Rechte vorbehalten.	- □ ×				
wb PS C:\Windows\ Die Richtlinie Die Aktualisie	system32> gpupdate /target:computer /force wird aktualisiert rung der Computerrichtlinie wurde erfolgreich abgeschlossen.					
Systeminformationen						
Datei Bearbeiten Ansicht ?						
Systemubersicht	Element	Wert				
Hardwareressourcen	Gesamter physischer Speicher	2,32 GB				
Komponenten	Verfügbarer physischer Speicher	622 MB				
Solution	Gesamter virtueller Speicher	2,97 GB				
	Verfügbarer virtueller Speicher	1,00 GB				
	Größe der Auslagerungsdatei	662 MB				
	Auslagerungsdatei	C:\pagefile.sys				
	Kernel-DMA-Schutz	Aus				
	Virtualisierungsbasierte Sicherheit	Wird ausgeführt				
	Virtualisierungsbasierte Sicherheit – erforderliche Sicherheitseigenschaften	Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz				
	Virtualisierungsbasierte Sicherheit – verfügbare Sicherheitseigenschaften	Allgemeine Virtualisierungsunterstützung, Sicherer Start, DMA-Schutz,				
	Virtualisierungsbasierte Sicherheit – konfigurierte Dienste	Credential Guard, Durch Hypervisor erzwungene Codeintegrität				
	Virtualisierungsbasierte Sicherheit – ausgeführte Dienste	A finite sector and and an				
	Es wurde ein Hypervisor erkannt. Features, die für Hyper-V erforderlich sind,	Nicht verfugbar				
Su	:hen nach:	Suchen Suche schließen				
	Nur ausgewählte Kategorie durchsuchen 🛛 Nur Kategorienamen durchsuchen					

Also initialisiere ich den Reboot. MSInfo zeigt nun einen laufenden Credential Guard:



Systeminformationen		
Datei Bearbeiten Ansicht ?		
Systemübersicht	Element	Wert
Hardwareressourcen	Gebietsschema	Deutschland
Komponenten	Hardwareabstraktionsebene	Version = "10.0.17763.1007"
Softwareumgebung	Benutzername	Nicht verfügbar
	Zeitzone	Mitteleuropäische Zeit
	Installierter physischer Speicher (RAM)	2,00 GB
	Gesamter physischer Speicher	2,00 GB
	Verfügbarer physischer Speicher	798 MB
	Gesamter virtueller Speicher	2,62 GB
	Verfügbarer virtueller Speicher	1,44 GB
	Größe der Auslagerungsdatei	640 MB
	Auslagerungsdatei	C:\pagefile.sys
	Kernel-DMA-Schutz	Aus
	Virtualisierungsbasierte Sicherheit	Wird ausgeführt
	Virtualisierungsbasierte Sicherheit – erforderliche Sicherheitseigenscha	Allgemeine Virtualisierungsunterstützung
	Virtualisierungsbasierte Sicherheit – verfügbare Sicherheitseigenschaften	Allgemeine Virtualisierungsunterstützung
	Virtualisierungsbasierte Sicherheit – konfigurierte Dienste	Credential Guard, Durch Hypervisor erzy
	Virtualisierungsbasierte Sicherheit – ausgeführte Dienste	Credential Guard, Durch Hypervisor erzv
	Unterstützung der Geräteverschlüsselung	Nicht verfügbar

Und wie entwickelt sich dessen Hunger auf Arbeitsspeicher? Das soll ein keines PowerShell-Script aufzeigen:

```
do {
    $wert = Get-Process -Name LsaIso | Select-Object -Property `
        @{ n="Zeit" ; e={ Get-Date -Format 'HH:mm:ss' } },
        @{ n="WorkingSet [kb]" ; e={ [int] ($_.workingset / 1024) } }

$wert | Export-Csv -Path .\LSAISO-Monitor.csv -Delimiter ';' -NoTypeInformation -Append
$wert
Start-Sleep -Seconds 15
} while ($true)
```

Ich starte das Script und lass den Server arbeiten:

```
LSAISO-Monitor.ps1 X
   1 ⊡do {
              $wert = Get-Process -Name LsaIso | Select-Object -Property`
    @{ n="Zeit" ; e={ Get-Date -Format 'HH:mm:ss' } }
    @{ n="WorkingSet [kb]"; e={ [int] ($_.workingset / 1024) } }
   2
   3
   4
   5
              $wert | Export-Csv -Path .\LSAISO-Monitor.csv -Delimiter ';' -NoTypeInformation -Append
   6
              $wert
              Start-Sleep -Seconds 15
   8
       } while ($true)
   9
PS C:\Users\stephan-T1\Desktop> C:\Users\stephan-T1\Desktop\LSAISO-Monitor.ps1
Zeit
            WorkingSet [kb]
08:49:58
08:50:12
                            4208
                            4208
```

Nach einiger Zeit hole ich mir die erzeugte CSV-Datei auf meinen Client und lasse Excel die Daten grafisch darstellen. Leider bläht sich LSAISO wieder auf:



	<del>ن</del> . ج	* \								LSAIS	O-Monitor.	csv - Excel
Dat	ei Start	Einfügen	Seitenlayo	ut Formeln	Daten	Überprüfer	n Ansicht	Hilfe 🏼 👰	Was	möchten Sie tun	?	
-	<b>.</b>	Calibri	∨ 11	VĂĂ	= = =	≣ ॐ •	ab c∉ Textumb	ruch		Standard	$\sim$	
Einfü	igen 💉	F <i>K</i> <u>U</u>	•	ð - <u>A</u> -	= = =	€ →	🖶 Verbinde	n und zentriere	en -	<b>₽ -</b> % ∞	€,0 ,00 ,00 →,0	Bedingte Formatierung - f
Zwisch	enablage 🗔		Schriftart			Au	Isrichtung		l⊇	Zahl		
N27	<b>v</b>		√ Jx									
	А	В		С	D	E	F	G		н	1	J
1	Zeit	t WorkingSe	et [kb]									
2	08:49:58	3	4208									
3	08:50:12	2	4208			Wo	orkingSet	[kb]				
4	08:50:27	7	4212	450000								
5	08:50:42	2	4212	400000								
6	08:50:57	7	4212	400000								
7	08:51:12	2	4212	350000								
8	08:51:27	7	4280	300000								
9	08:51:42	2	5532	250000			_					
10	08:51:57	7	6176	200000								
11	08:52:12	2	7216	150000								
12	08:52:27	7	7764	100000	_							
13	08:52:42	2	8056	50000								
14	08:52:57	7	8596	0 🧹								
15	08:53:12	2	8956		· ···? · ···?	5:0A 0	00 5.09	o.11 .5.13	·.^?	5:20 0:22		
16	08:53:27	7	9352	08.4 09	5. <sup>7</sup> 09 <sup>. PC</sup>	~0.0 ~0.3°	JO:2 - 77:3	12.0 22	2	23.00		
17	08:53:42	2	9836									
18	08:53:57	,	10128									
19	08:54:12	2	10684									

Die beiden Updates seit dem ersten Auftreten durch den Patch 2019-12 haben das Problem leider nicht gelöst. Mir bleibt nichts anderes über, als zu dem Workaround zurück zu kehren:

- Ich aktiviere die GPO mit der Device Guard Deaktivierung wieder.
- Danach wende ich die Richtlinie durch ein gpupdate an und starte den Server neu.
- Nun editiere ich den UEFI-Start und deaktiviere den UEFI-Lock des Device Guards auf der Konsole des Servers nach einem weiteren Neustart.

Es wird Zeit, den Hersteller zu informieren. Vielleicht habe ich ja einen Hinweis übersehen?

# <u>Zusammenfassung</u>

Auch wenn ich das Problem nicht zufriedenstellend lösen kann: Ich kenne nun die Ursache. Zusätzlich habe ich einen funktionalen Workaround gefunden.