

Prednosti održavanja Unimatrix-a

1. Pregled servera:

Serveri se pregledavaju periodično, interval pregleda se dogovara sa korisnikom. Tokom svakog pregleda se provjeravaju svi logovi vezani za server. (Application, Security, Setup, System) Kroz ove logove se može na vrijeme uočiti greške sistema ili pokušaja brute force napada. Takođe ako su hard diskovi ili drugi dijelovi hardvera problematični logovi nam pokazuju greške, tako da možemo na vrijeme reagovati.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view with 'Event Viewer (Local)' selected, showing categories like Custom Views, Windows Logs, Application, Security, Setup, System, Forwarded Events, Applications and Services Logs, Saved Logs, and Subscriptions. The main pane is titled 'Event Viewer (Local)' and shows an 'Overview and Summary' section. Below this is a 'Summary of Administrative Events' table with columns for Event Type, Event ID, Source, Log, Last hour, 24 hours, and 7 days. The table shows counts for Critical, Error, Warning, Information, Audit Success, and Audit Failure events. Below the table is a 'Recently Viewed Nodes' section with columns for Name, Description, Modified, and Created. The bottom section is 'Log Summary' with columns for Log Name, Size (Current), Modified, Enabled, and Retention Policy.

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
Error	-	-	-	0	20	59
Warning	-	-	-	0	10	14
Information	-	-	-	0	669	1,406
Audit Success	-	-	-	1,095	25,953	173,496
Audit Failure	-	-	-	0	42	287

The screenshot shows the Windows Event Viewer interface with a list of events selected. The main pane displays a table of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The selected event is an Error event with ID 10016 from the DistributedCOM source. Below the table, the details of this event are shown, including a description of the permission error and a 'More information' link. The bottom section shows the event's properties, including Log Name, Source, Event ID, Level, User, OpCode, and More information.

Level	Date and Time	Source	Event ID	Task C...
Information	25.05.2017, 07:56:52	Service Control Manager	7036	None
Information	25.05.2017, 07:56:52	Service Control Manager	7036	None
Information	25.05.2017, 07:56:52	Service Control Manager	7036	None
Error	25.05.2017, 07:56:51	DistributedCOM	10016	None
Information	25.05.2017, 07:56:51	Service Control Manager	7036	None
Information	25.05.2017, 07:56:50	Kernel-General	16	None
Information	25.05.2017, 07:56:50	Wsllogon	7001 (118)	
Information	25.05.2017, 07:49:38	Service Control Manager	7036	None

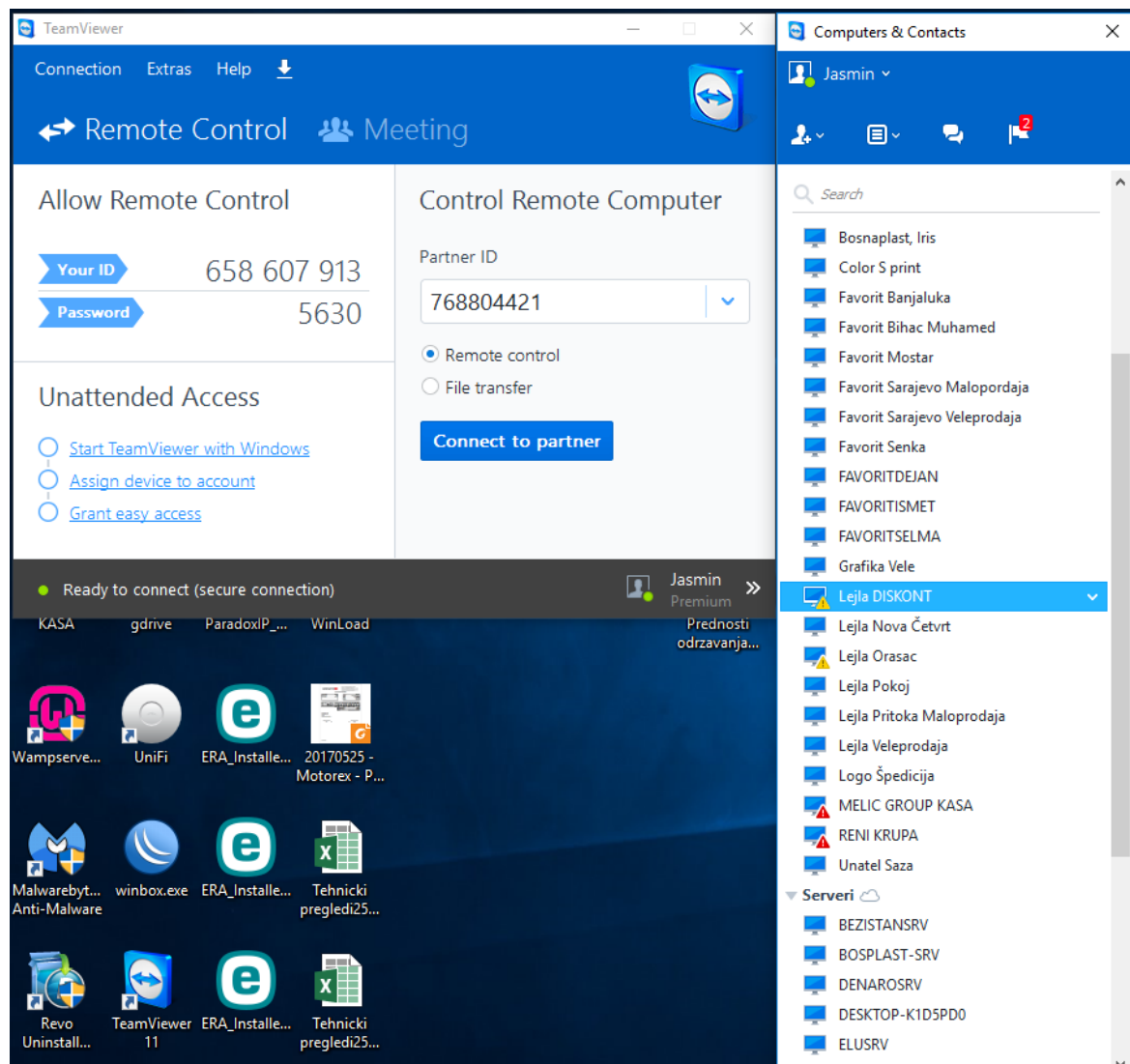
The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID {809F4F08-3594-4F07-8969-FC33CAE4919} and APPID {F72671A9-012C-4725-902F-2A4D32D05169} to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.

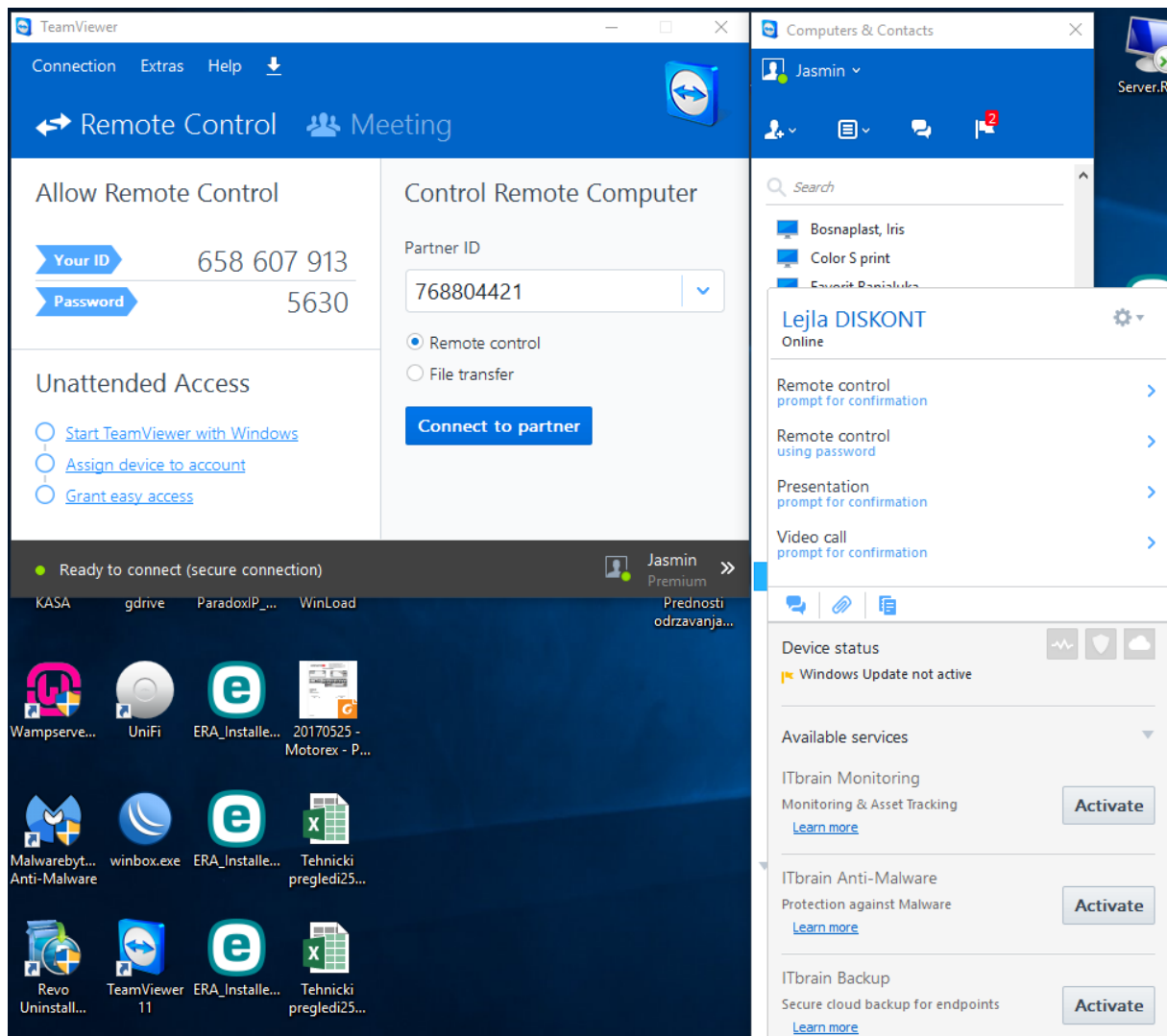
Log Name: System
Source: DistributedCOM
Event ID: 10016
Level: Error
User: SYSTEM
OpCode: Info
Logged: 25.05.2017, 07:56:51
Task Category: None
Keywords: Classic
Computer: UNIFFTP.rvtftp.domain
More information: [Event Log Online Help](#)

2. Kontrola računara kroz teamviewer:

Unimatrix posjeduje **licenciran teamviewer**, gdje se na svaki računar instalira teamviewer i omogućava daljinski pristup na korisnikove računare. Osim što omogućava instant pristup kod intervencija i problema koji korisnik može imati, teamviewer takodje ima konzolu koja obavještava nas kao servisere ako nešto nije uredu sa korisnikovim računarom te možemo na vrijeme reagovati. Klasične greske koje se dešavaju a uočljive su kroz ovaj sistem za praćenje su:

- isključeni update windows operativnog sistema ili ako update-i nisu ažurirani. (jako bitno za zaštitu od naprednih malvera kao što su kriptolokeri koje iskorištavaju sigurnosne propuste kod računara koji nisu na vrijeme ažurirana)
- Isključen ili ne ažuriran antivirus – često se zna desiti interna greška na antivirusu gdje usljed blokade sporednih servisa antivirus se isključi te ne pruža adekvatnu zaštitu.





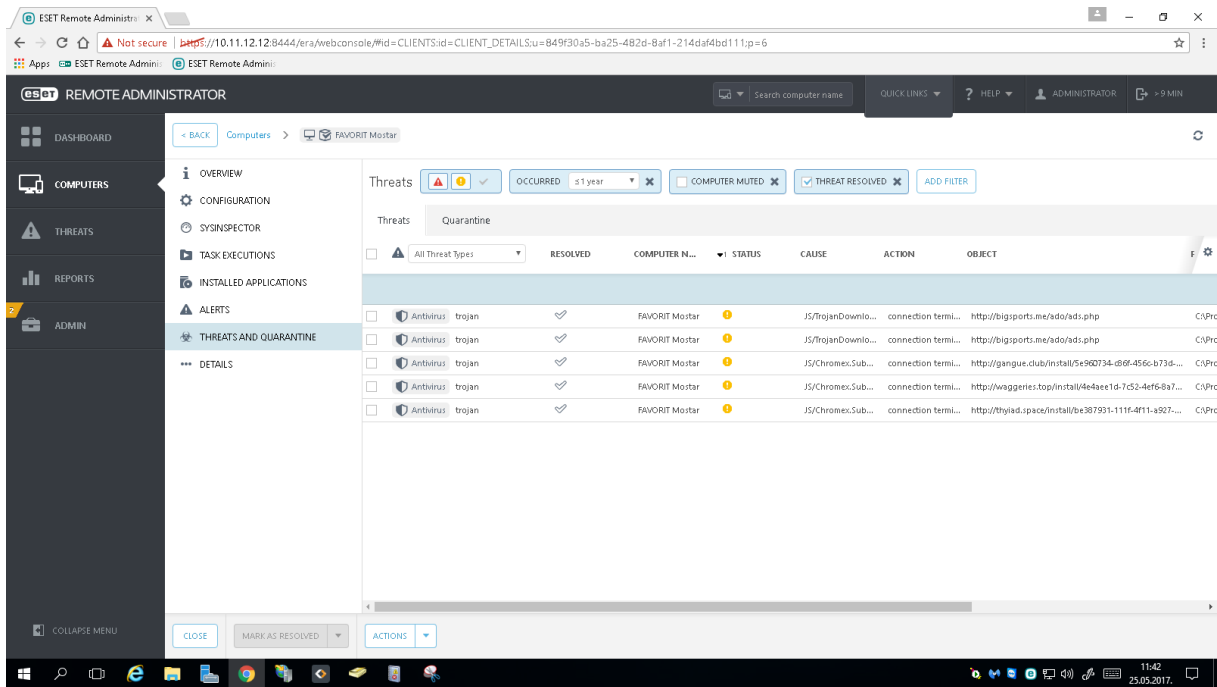
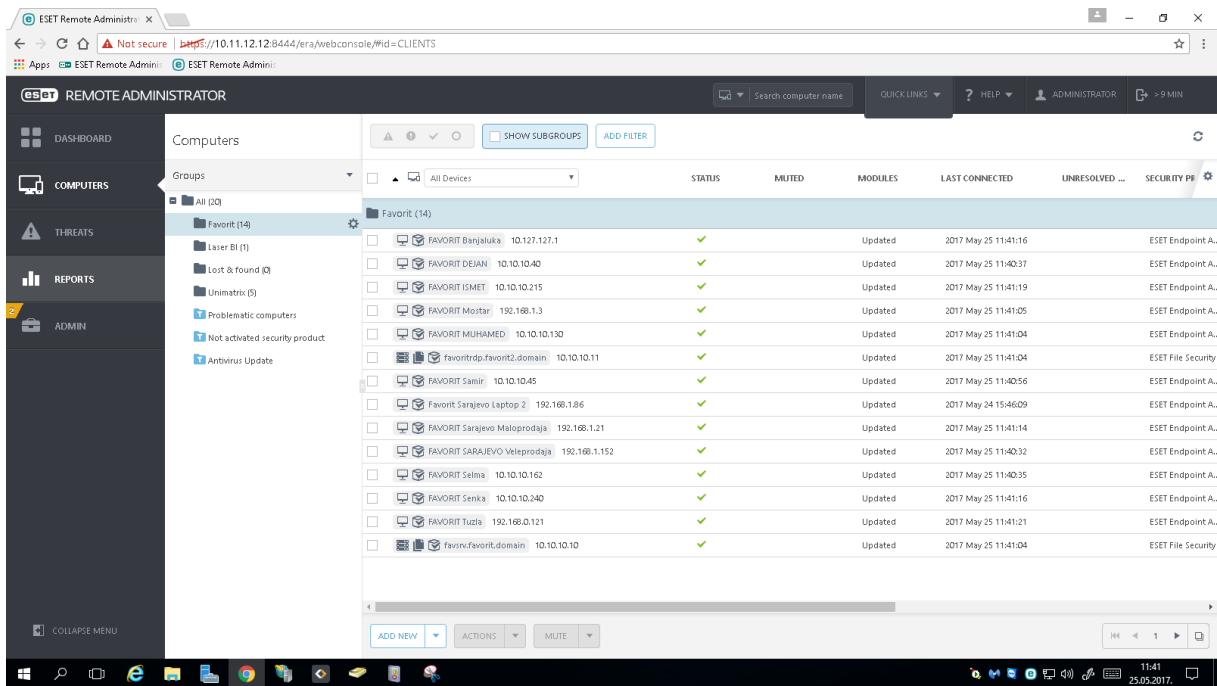
3. Praćenje i kontrola korisnika kroz ESET Remote Administrator

Ovaj sistem omogućava praćenje rada računara i optimizira rad antivirusnog sistema. Šta je jako bitno za ovaj sistem jesta da antivirus kod korisničkog računara kad se poveže sa serverom ESET Remote Administratora, je da apsolutno ni pod kojim uvjetima ne dopušta isključenje antivirusa stalno ili privremeno.

Svjedoci smo da korisnici instaliraju razno razne besplatne i krekovane programe koji su često zaraženi malwerima i zbog ne znanja da bi instalirali takav program isključe antivirus i nesvjesno zaraze malwerima kompletan sistem, koji može dovesti do sporijeg rada računara, pregrijavanje komponenti, i u najgorem sve češćem slučaju zaključati podatke gdje se kasnije od kupaca zahtjeva određen iznos novca da se podaci otključaju.

Jos jedna bitna prednost ovog sistema jeste da antivirus na korisnikovom računaru šalje sve aktivnosti antivirusa na Unimatrix server gdje se traži od administratora da pregleda svaku zabilježenu prijetnju.

Kroz pregled ovih prijetnji možemo odrediti koje je stranice korisnik posjećivao te na vrijeme prenijeti menadžmentu firme da upozori korisnika da ne posjećuje takve stranice na poslovnim računarima.



4. Secure FTP Backup

FTP Backup služi kao dodatni backup i nalazi se u prostorijama Unimatrix doo gdje je pod konstantnim nadzorom i provjerama od raznih sigurnosni prijetnji. Imali smo slučajeve gdje kompletna backup strategija kod korisnika zakaže te se ovo rješenje pokazalo kao pouzdano i odlično rješenje za vraćanje podataka poslovanja kao što su WAND i NIBIS.