

Ek Döküman No: AG.1.01 Cacti Yazılımı ile Ağ Trafik Takibi

Cacti Nedir ?

Cacti; network ağı üzerinde bulunan aktif cihazlarınızın bellek (ram), disk, ağ ve sistem yükü gibi bilgilerini grafiksel olarak web arayüzüyle sunan, komple bir sunucu çözümüdür. Bilgileri almak için snmp ve aldığı bu bilgileri grafiksel olarak yazmak için rrdtool araçlarını kullanır.

Cacti'yi çalıştırmak için aşağıdaki paketleri sisteminize kurmalısınız.

- Apache
- PHP
- NET-SNMP
- RRDTOOL

Cacti açık kaynak bir yazılımdır ve bu nedenle Linux Unix türevi sistemler üzerinde çalışır.

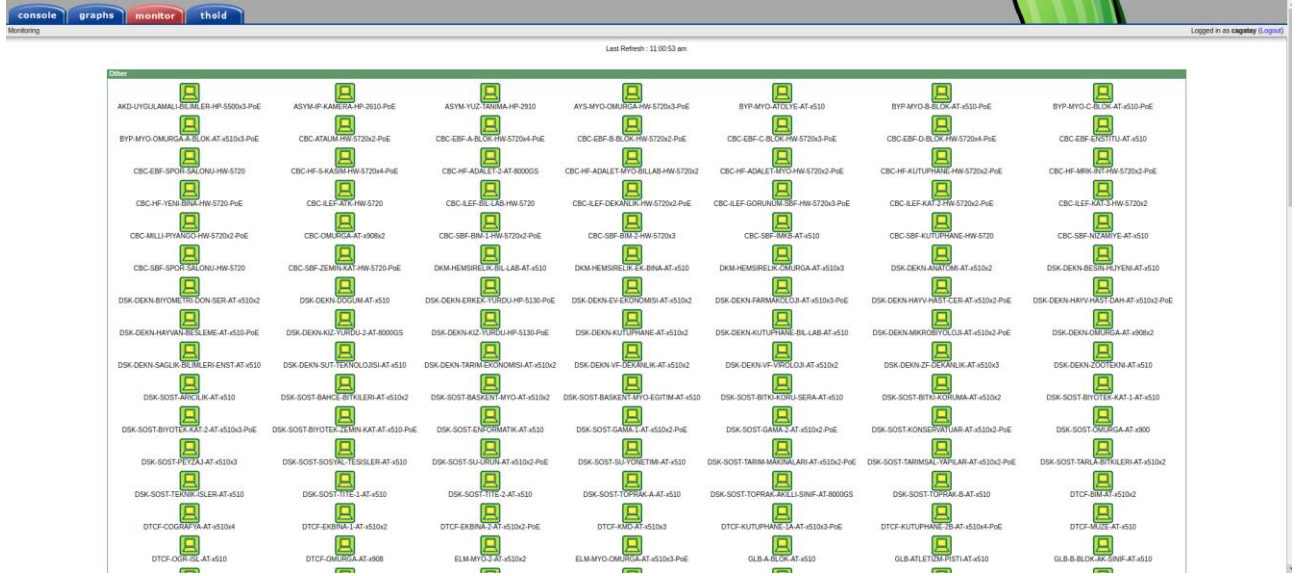
Cacti sistem ve ağ cihazları izleme yazılımı, SNMP (Simple Network Management Protocol) protokolünü kullanarak, izlemek istenen cihazdan aldığı snmp sorgularının cevabına göre grafikler oluşturarak sistem ve ağ cihazlarını izlememizi(monitoring) sağlar. SNMP protokolü sayesinde ağ trafiği, port trafiği, kullanıcı, sistem yükü, disk kapasitesi, bellek kullanımı vb. gibi bilgileri kolay anlaşılır bir grafik ekranla sunar.

Cacti sistem ve ağ cihazları izleme yazılımı, grafik ekran olarak RRdTool, veri tabanı olarak ise MySQL kullanır. Php web yazılım dili kullanılarak yazılmıştır. İstenildiğinde özelleştirilebilir.

Grafik ekrandaki veri kaynaklarını ise, zamanlanmış görevlerde tanımlanan script sayesinde 5 dk lık sorgular sonucunda veritabanına yazacaktır. Grafik ekranlardaki bilgiler ise veri tabanından güncellenerek son ana kadar olan bilgiyi verecektir.

RRDTool grafik aracını kullanır. Oluşturulan bu grafiklerin birkaç şekilde gösterimleri mevcuttur. Ön izleme, hiyerarşik veya ağaç(tree) yapısı şeklinde görüntülenebilir.

Ek Döküman No: AG.1.01 Cacti Yazılımı ile Ağ Trafik Takibi



Resim 1

Resim 1 de görülen ekran Cacti'nin monitor ekranıdır. İlk kurulumda bu ekranı göremeyiz çünkü bu ekran bir plug-in dir. Cacti kurulumundan sonra ayrıca kurulması gerekmektedir. Bu ekranda mevcut ağ cihazlarımızın o anda up/down durumlarını yani çalışıp çalışmadıklarını görebiliriz. Çalışan cihazlar yeşil renkte, çalışmayan cihazlar kırmızı renkte gösterilir.

Description	ID	Graphs	Data Sources	Status	In State	Hostname	Current (ms)	Average (ms)	Availability
AKD-UYGULAMALI-BILGILER-HP-5500x3-PxE	506	145	145	Up	28d 5h 28m	10.129.10.1	4.27	10.59	99.78
ASYM-IP-KAMERA-HP-2610-PxE	790	51	51	Up	117d 5h 37m	10.122.10.3	3.34	7.14	99.99
ASYM-OMURG.A-HP-5412x3-PxE	659	496	496	Up	117d 5h 37m	10.122.10.1	1.84	16.5	99.94
ASYM-YUZ-TANIMA-HP-2910	789	48	48	Up	117d 5h 37m	10.122.10.2	5.58	6.17	99.98
AYS-MYO-OMURG.A-HP-5720x3-PxE	661	146	146	Up	28d 2h 52m	10.123.10.1	8.46	12.01	99.7
BYP-MYO-ATOLYE-AT-4510	787	50	50	Up	6d 27h 7m	10.109.10.6	12.71	8.24	99.76
BYP-MYO-B-BLOK-AT-4510x3-PxE	423	50	50	Up	49d 20h 23m	10.109.10.3	7.67	9.86	99.88
BYP-MYO-C-BLOK-AT-4510x3-PxE	424	50	50	Up	49d 18h 13m	10.109.10.4	7.67	9.87	99.77
BYP-MYO-OMURG.A-BLOK-AT-4510x3-PxE	422	146	146	Up	51d 12h 38m	10.109.10.1	7.12	9.97	99.88
BYP-MYO-SANAL-SINIF-AT-4510	777	50	50	Up	8d 13h 1m	10.109.10.2	7.27	8.15	97.15
CBC-ATAUM-HW-5720x3-PxE	564	98	98	Up	28d 5h 27m	10.111.10.11	13.84	6.57	99.58
CBC-ESF-A-BLOK-HW-5720x4-PxE	556	194	194	Up	28d 5h 27m	10.111.10.5	3.63	6.39	99.68
CBC-ESF-B-BLOK-HW-5720x3-PxE	565	98	98	Up	28d 5h 27m	10.111.10.4	7.65	8.69	99.85
CBC-ESF-C-BLOK-HW-5720x4-PxE	538	146	146	Up	28d 5h 28m	10.111.10.3	3.97	5.95	99.59
CBC-ESF-D-BLOK-HW-5720x4-PxE	554	194	194	Up	28d 5h 27m	10.111.10.2	4.88	6.19	99.83
CBC-ESF-ENSTITU-AT-4510	212	50	50	Up	28d 5h 28m	10.111.10.15	4.37	6.25	99.61
CBC-ESF-SPOR-SALONU-HW-5720	537	50	50	Up	2d 1h 18m	10.111.10.27	13.96	6.09	96.5
CBC-HF-S-KASIM-HW-5720x4-PxE	558	194	194	Up	28d 5h 27m	10.111.10.6	3.67	7.2	99.92
CBC-HF-ADALET-3-AT-8000G5	499	48	48	Up	28d 5h 28m	10.111.10.14	3.23	8.79	79.01
CBC-HF-ADALET-MYO-BILAB-HW-5720x2	563	98	98	Up	28d 5h 27m	10.111.10.28	4.22	7.75	99.92
CBC-HF-ADALET-MYO-HW-5720x2-PxE	562	98	98	Up	28d 5h 27m	10.111.10.9	3.49	6.31	99.92
CBC-HF-KUTUPHANE-HW-5720x3-PxE	560	98	98	Up	28d 5h 27m	10.111.10.8	4.57	6.14	99.92
CBC-HF-MRK-AT-HW-5720x2-PxE	559	98	98	Up	28d 5h 27m	10.111.10.7	6.57	7.31	99.92
CBC-HF-YENI-BINA-HW-5720-PxE	561	50	50	Up	19d 22h 17m	10.111.10.10	3.83	6.81	99.76
CBC-ILEF-ATK-HW-5720	548	50	50	Up	4d 18h 2m	10.111.10.20	6.2	5.99	97.87
CBC-ILEF-BIL-LAB-HW-5720	550	50	100	Up	28d 5h 28m	10.111.10.23	3.57	6.49	99.77
CBC-ILEF-DEKANLIK-HW-5720x3-PxE	607	98	98	Up	28d 5h 27m	10.111.10.24	3.44	6.87	98.63
CBC-ILEF-GORUNUM-SBF-HW-5720x3-PxE	549	146	146	Up	28d 5h 28m	10.111.10.22	3.42	6.11	99.57
CBC-ILEF-KAT 2-HW-5720x3-PxE	551	98	98	Up	28d 5h 28m	10.111.10.26	3.49	6.09	99.93
CBC-ILEF-KAT 3-HW-5720x2	552	98	98	Up	28d 5h 28m	10.111.10.21	4.47	6.17	99.66
CBC-KAMERA-OMURG.A-AT-4908	661	0	0	Down	28d 5h 27m	10.111.10.100	0	0	100
CBC-MILLI-PYKINGO-HW-5720x3-PxE	566	98	98	Up	28d 5h 27m	10.111.10.29	5.13	7.03	99.58
CBC-OMURG.A-AT-4908x2	173	36	36	Up	28d 5h 28m	10.111.10.1	5.43	7.24	99.9

Resim 2

Burada görülen ekranda da varolan tüm cihazlarımızın listesini görebilir spesifik bir cihazı arayabilir, ağ cihazlarının çalışıp çalışmadıklarını, çalışıyorlarsa ne kadar zamandan beri aktif olduklarını tespit edebiliriz. Aynı zamanda sağ üst köşede yer alan “Add” butonuyla yeni bir ağ cihazını sisteme ekleyebiliriz. Sol tarafta bulunan menüden ise grafik yönetimi, grafik ağacı, plug-in yönetimi, ayarlar gibi sekmelere gidebiliriz.

Ek Döküman No: AG.1.01 Cacti Yazılımı ile Ağ Trafik Takibi



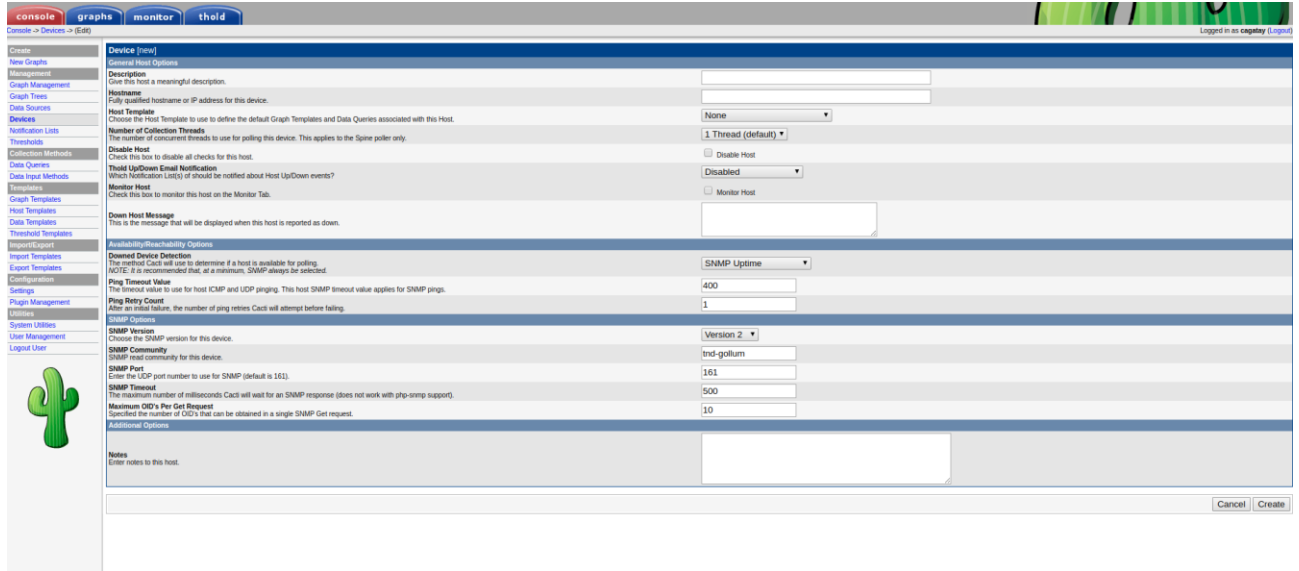
Resim 3

Sıradaki resimde de Cacti'nin "graphs" sekmesini görüyoruz. Burası bizler için çok önemli çünkü sistemde varolan tüm ağ cihazlarına ait grafikler burada yer almaktadır. Yukarıdaki filter sayesinde istediğimiz cihazının, dilediğimiz zaman aralığında yada spesifik bir anda hangi portunda nasıl bir grafik oluşturduğunu en basit ve anlaşılır şekilde burada görebiliriz. Grafiklerde Yeşil olan kısımlar inbound, mavi kısımlar ise outbound trafik grafikleridir.

Graphs ekranının sol tarafında ise bizim oluşturduğumuz Grafik ağacını görebiliriz. Bu grafik ağacı mevcut topolojimizin yapısını da bizlere göstermektedir.

Grafiklerin üzerlerinde yer alan açıklama bize o portun ne olduğu bilgisini verir. Bu açıklama ağ cihazı üzerinde yer alan port description bilgisidir ve Cacti snmp ile bu bilgiyi çekerek o portun grafiği üzerine yazar.

Ek Döküman No: AG.1.01 Cacti Yazılımı ile Ağ Trafik Takibi



The screenshot displays the Cacti web interface for adding a new device. The interface is organized into a sidebar on the left and a main content area. The sidebar includes navigation links such as 'console', 'graphs', 'monitor', and 'threshold'. The main content area is titled 'Device [new]' and contains several sections for configuration:

- General Host Options:** Includes fields for 'Description', 'Hostname', 'Host Template', 'Number of Collection Threads', 'Disable Host', 'Threshold Up/Down Email Notification', 'Monitor Host', and 'Down Host Message'.
- Advanced Device Detection:** Includes a 'SNMP Uptime' dropdown, 'Ping Timeout Value', 'Ping Retry Count', and 'SNMP Version'.
- SNMP Community:** Includes a 'SNMP Community' dropdown, 'SNMP Port', and 'SNMP Timeout'.
- SNMP Timers:** Includes a 'Maximum OID's Per Get Request' field.

At the bottom of the form, there is a 'Notes' section and 'Cancel' and 'Create' buttons.

Resim 4

Daha önce de değindiğimiz devices ekranının sol üst köşesinde yer alan “Add” butonuna bastığımız zaman yukarıdaki cihaz ekleme ekranına geliriz. Burada cihazımızın açıklaması,hostname bilgisi, monitor edip edilmeyeceği, snmp community bilgisi gibi bilgileri girerek sağ altta “create” butonuna bastığımızda -eğer girdiğimiz bilgilerde bir yanlışlık yoksa- cihazımız sisteme eklenecektir.Ardından cihazla ilgili grafikler oluşturularak grafik ağacında yerleri belirlenerek graph management ekranı ile ilgili yere import edilebilirler.