eScan™
Anti-Virus & Content Security

eScan for NAS

www.escanav.com

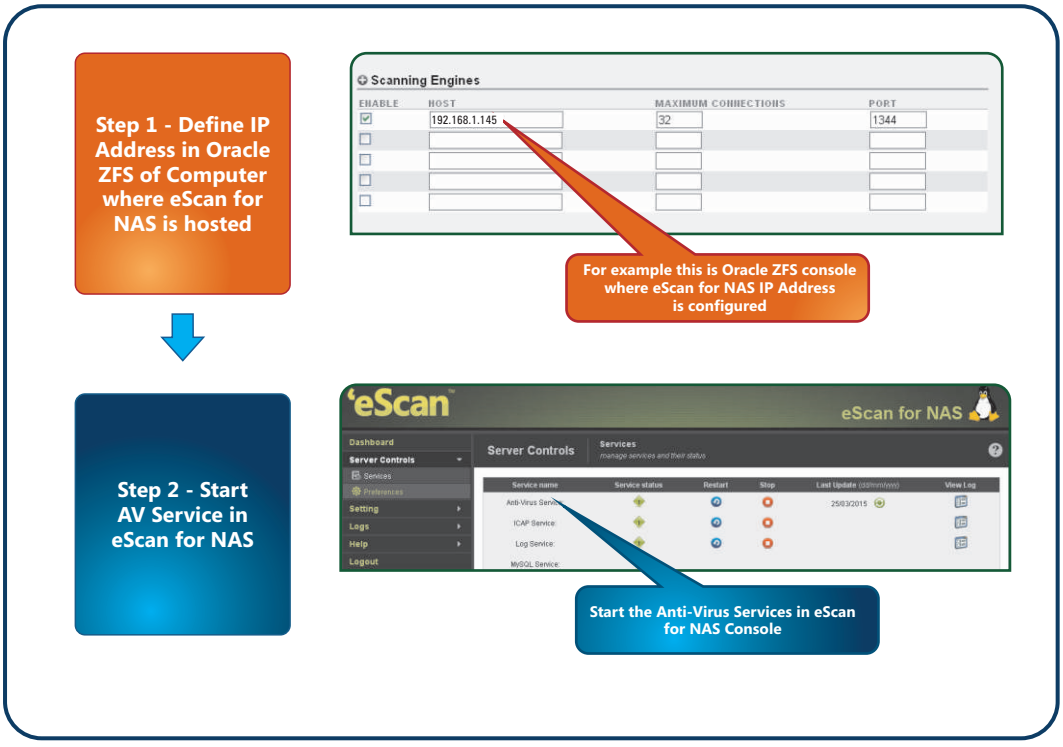
eScan for NAS

Data is one of the most valuable assets of any enterprise and it must be readily available to the authorized employees, for this purpose companies have started integrating Network Attached storage devices into their networks for storing data essential for business continuity. NAS or Network Attached Storage is a type of dedicated file server that provides centralized, consolidated disk storage to LAN users through a standard Ethernet connection.

Any malware attack on NAS Server can cause irrecoverable loss to critical data stored on them. It is of greater importance to protect all data stored on NAS Servers. eScan for NAS provides protection to the data stored on them through its malware protection engine and advanced heuristics and AV technology that facilitates faster, scalable and reliable content scanning, helping organizations protect their data and storage systems against ever growing threat landscape. Malware definitions and AV engine is updated using update servers located worldwide ensuring total security against viruses, and blended threats.

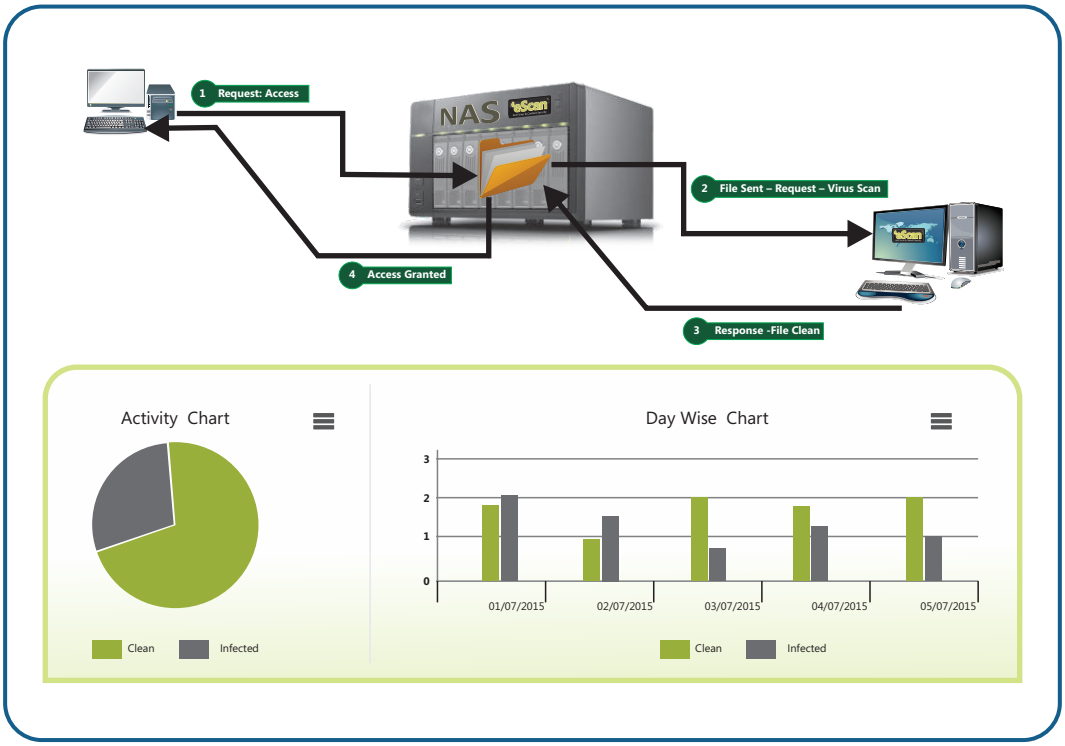
How it Works

For securing your NAS Servers, first you need to install eScan for NAS with integrated ICAP Services on any computer on the network. After installation, configure scanning engine details (eScan for NAS) such as IP address, Maximum Connections allowed and Port Number in your Oracle ZFS storage appliance control panel. Once the configuration is over, start AV Services in eScan for NAS.It will act as an external scanning engine.



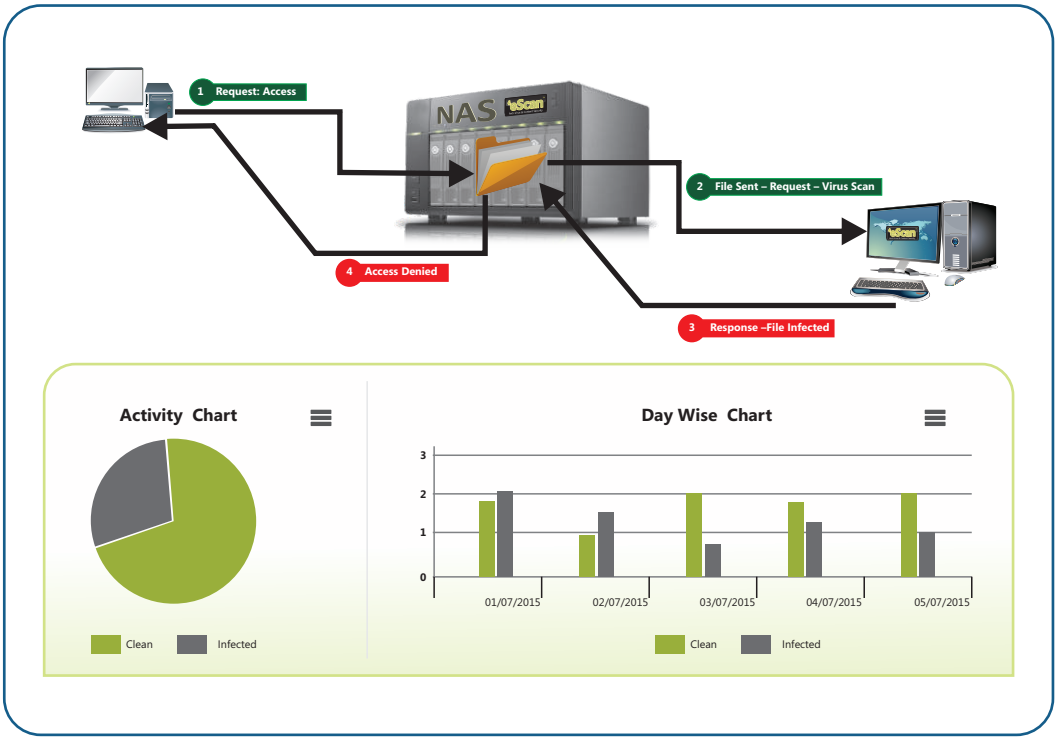
This will start the scanning services instantly. However, the scanning of any object dropped /opened/ modified on the NAS server will take place only when a scanning request is issued by Oracle ZFS to eScan for NAS. The file is sent to eScan for NAS by the Oracle ZFS storage appliance and virus scanning service is initiated instantly. The results- File is infected or File is Clean is then sent back to Oracle ZFS to take pre-configured actions such as Access Granted (in case the File is clean), or Access Denied (in case the File is infected), or Quarantine File (in case the file is infected and access is denied by Oracle ZFS).

How it Works – When the file is sent to eScan for NAS and is found ***Clean***

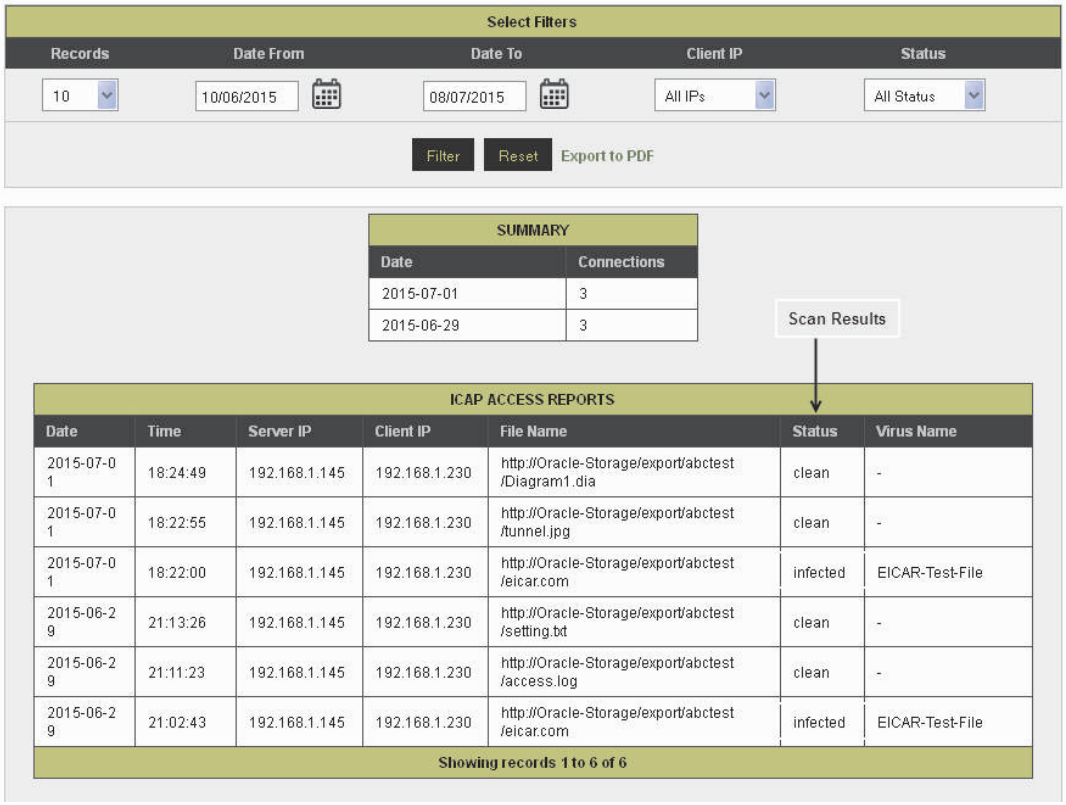


Files are saved on NAS Server, whenever a File Access request is received by the NAS Box, the file is sent to eScan for NAS for Virus scanning. After scanning if the File is found clean, access is granted to the user or denied in case the file is infected. Access Granted or Denied and conditions for the same are configured in Oracle ZFS storage appliance control panel. After receiving the results received from eScan for NAS, corresponding command is executed.

How it Works – When the file is sent to eScan for NAS and is found ***Infected***



eScan also maintains daily reports in Activity Chart and Day Wise Graphs for the number of Files Scanned and found clean or infected. It also generates a comprehensive report for every file scanned.



Select Filters

Records	Date From	Date To	Client IP	Status
10	10/06/2015	08/07/2015	All IPs	All Status

Filter Reset Export to PDF

SUMMARY

Date	Connections
2015-07-01	3
2015-06-29	3

Scan Results

ICAP ACCESS REPORTS

Date	Time	Server IP	Client IP	File Name	Status	Virus Name
2015-07-01	18:24:49	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/Diagram1.dia	clean	-
2015-07-01	18:22:55	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/tunnel.jpg	clean	-
2015-07-01	18:22:00	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/eicar.com	infected	EICAR-Test-File
2015-06-29	21:13:26	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/setting.txt	clean	-
2015-06-29	21:11:23	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/access.log	clean	-
2015-06-29	21:02:43	192.168.1.145	192.168.1.230	http://Oracle-Storage/export/abctest/eicar.com	infected	EICAR-Test-File

Showing records 1 to 6 of 6

The generated report can be filtered by the Administrator on the basis of Records maintained, specific dates and time, Client IP or the Status (Infected or Clean). It also displays the name of Virus that had infected the file.

System Requirement

CPU: 2GHz Intel™ Core™ Duo processor or equivalent

Memory: 2GB RAM