

ARCON|PAM
Specction V4.8.5.0_U21

Table of Contents

1	Introduction	5
1.1	Features	5
1.2	Spection Architecture	5
2	Spection Installation	6
2.1	Pre-requisites	6
2.1.1	Dependent Installations	6
2.2	PackageStructure.....	7
2.2.1	Copying the package.....	7
2.3	ARCON Spection Hosting.....	8
2.3.1	ACMO Hosting.....	8
2.3.1.1	Hosting Spection UI.....	8
2.3.1.2	Hosting Spection API	9
2.3.1.3	DB Settings configuration for Spection API	9
2.3.2	Independent Hosting	9
2.3.2.1	Hosting ARCON SpectionUI	9
2.4	Configurations.....	10
2.4.1	SpectionUI Configuration.....	10
2.4.2	SpectionAPI Configuration	10
2.4.3	ARCOSClientManagerOnline Configuration	11
3	Accessing ARCON PAM Spection..	12
3.1	Spection Features	13
3.1.1	Entities of ARCON PAM.....	13
3.1.2	Privilege Based Access.....	15
3.1.3	Scheduling Report.....	17
3.1.3.1	Create a scheduler	17
3.1.3.2	View Configured scheduler	19
3.1.3.3	SMTP Configuration	20
3.1.4	Filtering	20
4	Spection Dashboard.....	24
4.1	Widgets	24
4.2	Graphs	24
4.3	Access to all reports	27
5	Spection Reports	28

5.1	LOB Report	28
5.1.1	LOB Report Generation.....	28
5.2	User Group Report	30
5.2.1	User Group Report Generation.....	31
5.3	Service Group Report.....	33
5.3.1	Service Group Report Generation	33
5.4	User Report	36
5.4.1	User Report Generation.....	36
5.5	Service Report	39
5.5.1	Service Report Generation.....	40
5.6	Session Report.....	42
5.6.1	Session Report Generation	45
5.7	Command Report.....	48
5.7.1	Command Report Generation.....	50
5.8	Process Report	53
5.8.1	Process Report Generation.....	54
5.9	Outside Access Report.....	58
5.9.1	Outside Access Report Generation	58

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.

Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Copyright Notice

Copyright © 2022 ARCON All rights reserved.

ARCON retains the right to make changes to this document at any time without notice. ARCON makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact

You can directly contact us with sales-related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Introduction

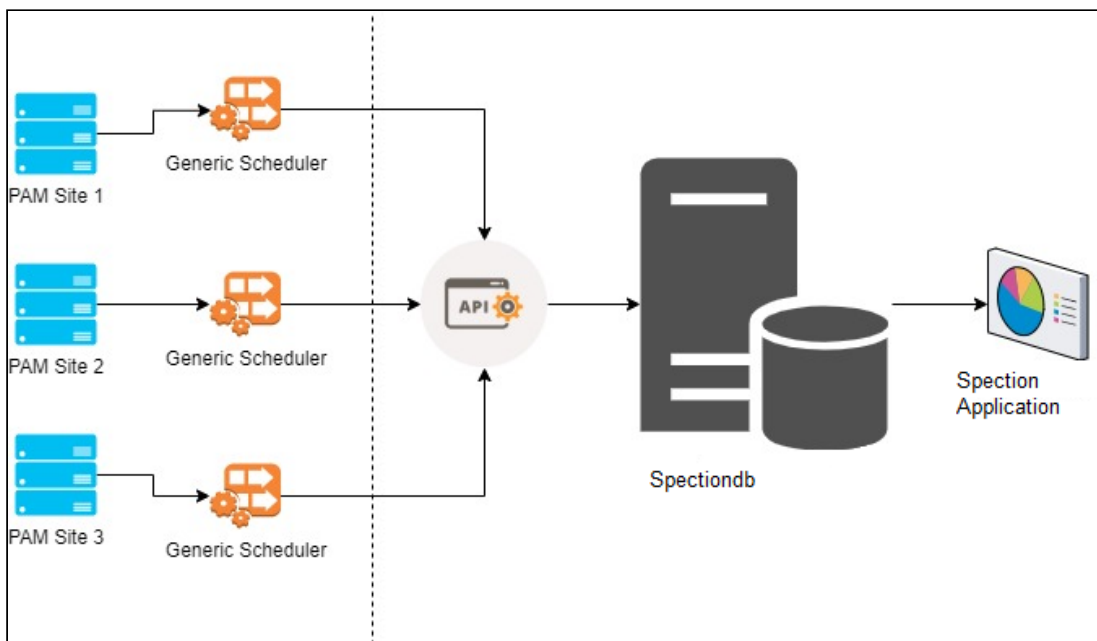
The report generation process encompasses quite a wide range of requirements that can be very subjective and it becomes a difficult task to manage and monitor the activities performed by everyone. ARCON|Spection is a dynamic report builder that allows searching as well as filtering capabilities to derive a detailed compilation of all activities. It also provides entity wise views, so you can see the activities performed from a command level, session level, user level, or even a group level view.

1.1 Features

- **Bespoke Reports**
Spection gives complete control to filter the data to suit the user's tailor-made requirements, by providing a completely dynamic template.
- **Comprehensible Representation**
Displays extensive data in the form of detailed and neat pictorial formats which include statistics, graphs, and tabular grid for a report
- **Compact Size**
It runs on a data warehousing solution that gives it a lightweight feel and speed.
- **Easily Downloadable**
Users can export these reports in .csv, .pdf, and .xlsx file formats.

1.2 Spection Architecture

Spection is a reporting tool database and can consist of multiple PAM Instances. Each PAM Instances should have a generic schedule service installed and the service should point to the respected PAM Database. Generic Scheduler Service in PAM should point to the API Server of Spection.



2 Spection Installation

This document will guide you through the steps involved in deployment for the **ARCON Privileged Access Management (PAM) Spection**. The following steps are to be followed for the successful deployment of ARCON PAM Spection in your environment.




2.1 Pre-requisites

Before installing the **ARCON PAM Spection**, you should check the points enlisted below to ensure that your environment meets the minimum installation requirement for the ARCON PAM Spection.

- Pre-configuration: Spection & Knight Analytics is done.
- ARCON PAM Spection Package.
- Firewall should be enabled for Spection UI URL and Spection API URL from end user.
- SQL server enterprise edition (full text support)
- NET Core Hosting Bundle version 2.2.6
- Minimum Hardware Requirements:
 - a. CPUs with AVX support minimum 6 cores
 - b. 16 GB RAM and additional 16GB on standby
 - c. Drive 200GB
 - d. OS should be Windows Server 2012 +

2.1.1 Dependent Installations

- Install 41 IIS roles
- Data warehouse setup
Please refer to the Data warehouse document for further understanding.
- Double click on dotnet-hosting-2.2.6-win.exe

Name	Date modified	Type	Size
 SpectionAPI	7/13/2020 6:19 PM	File folder	
 SpectionUI	7/13/2020 6:26 PM	File folder	
 dotnet-hosting-2.2.6-win.exe	8/7/2020 7:03 PM	Application	98,400 KB

- The following popup will be displayed.



- Select the checkbox I agree to the license terms and conditions.
- Click Install
- Click **Finish**.

2.2 PackageStructure

2.2.1 Copying the package

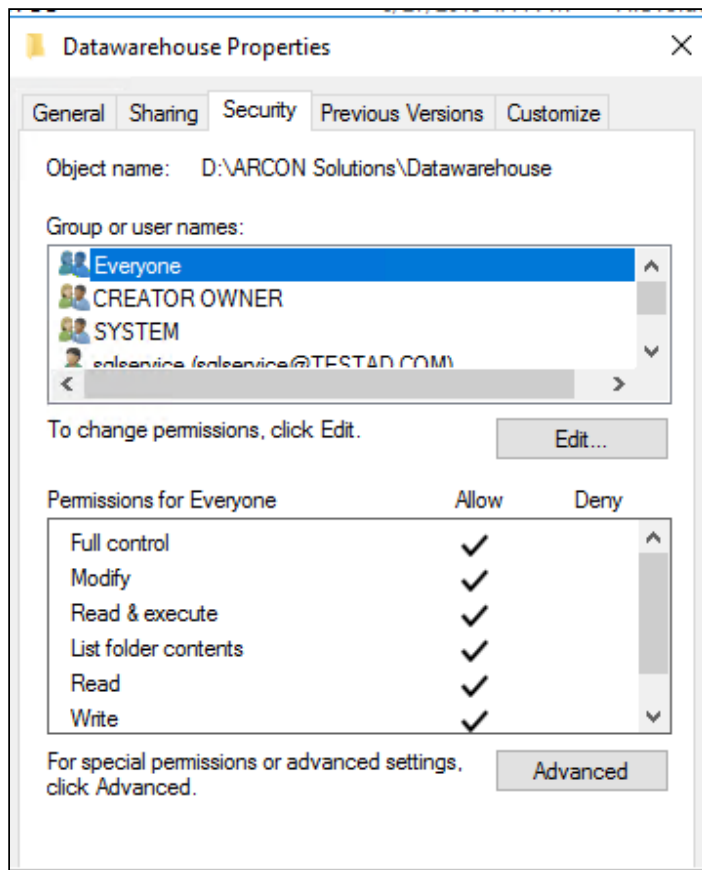
This section provides information about how to configure ARCON PAM Spection on IIS Manager.

Use the following steps to configure **ARCON Spection**:

1. Create **Spection** folder on ARCON Solutions path e.g. <Drive>:\ARCON Solutions\Spection
2. Copy the **Spection.zip** and unzip files to the above drive location created i.e. <Drive>:\ARCON Solutions\Spection
3. Unzip the **Spection** file.
4. Kindly check for the **SpectionAPI** folder e.g. <Drive>:\ARCON Solutions\Spection, everyone has permission at the folder level.
5. Inside Spection folder, we will have SpectionUI folder and SpectionAPI folder.

Name	Date modified	Type	Size
SpectionAPI	7/13/2020 6:19 PM	File folder	
SpectionUI	7/13/2020 6:26 PM	File folder	
dotnet-hosting-2.2.6-win.exe	8/7/2020 7:03 PM	Application	98,400 KB

Give full permission to all folders of Knight and Spection.



2.3 ARCON Spection Hosting

Spection can be hosted in two ways

1. ACMO Hosting
2. Independent Hosting

2.3.1 ACMO Hosting

2.3.1.1 Hosting Spection UI

This section provides information about how to host ARCON SpectionUI

Use the following steps to add the application pool for ARCON SpectionUI.

1. Goto **Start** button and type **run**.
2. In **run** window type '**inetmgr**'. The **Internet Information Services (IIS) Manager** window opens.
3. Add **Application Pool- SpectionUIPool**.
4. The .NET CLR version should be set to **No Managed Code**.
5. Set Managed pipeline mode to **integrated**.
6. Right-click ACMO site on IIS.
7. Add application.
8. Give alias name as SpectionUI.
9. Set ApplicationPool- SpectionUIPool.

10. Bind it pointing to SpectionUI.
11. Enable preload checkbox should be ticked.

2.3.1.2 Hosting Spection API

This section provides information about how to host ARCON SpectionAPI

Use the following steps to add the application pool for ARCON SpectionAPI.

1. Goto **Start** button and type **run**.
2. In **run** window type '**inetmgr**'. The **Internet Information Services (IIS) Manager** window opens.
3. Add **Application Pool- SpectionAPIPool**.
4. The .NET CLR version should be set to **No Managed Code**.
5. Set Managed pipeline mode to **integrated**.
6. Right-click ACMO site on IIS.
7. Add application.
8. Give alias name as SpectionAPI
9. Select ApplicationPool-SpectionAPIPool.
10. Bind it pointing to SpectionAPI folder.
11. Enable preload checkbox should be ticked.

2.3.1.3 DB Settings configuration for Spection API

1. Goto <Drive>:\ARCON Solutions\Spection\SpectionAPI\DBSetting folder.
2. Double click on '**ARCOSDBSettingCreator.exe**'
3. The **ARCON PAM Database DBSettings.ini File Creator** window opens. Enter the following details:
Connection Details (Primary)
 - a. **Server IP**– Enter the address where the Spection Database is located
 - b. **Server Port**– Enter the port on which the ARCON PAM Spection Database will listen (Default port is - 1433)
 - c. **Server Name**– Enter the name of the server / IP address.
 - d. **User Name**– Enter the ARCON PAM Spection database name.
 - e. **User Password**– Enter the ARCON PAM Spection database password.

Click on **Generate ini file** button, to generate the ini file. The **ini** file is generated inside the DBSetting folder.

2.3.2 Independent Hosting

This section provides information about how to host ARCON Spection UI and API independently on same port.

1. Right-click on the IIS site.
2. Add application.
3. Give alias name as Spection.
4. Bind it pointing to SpectionUI folder in the package.
5. Enable preload checkbox should be ticked.

2.3.2.1 Hosting ARCON SpectionUI

This section provides information about how to configure ARCON SpectionUI

Use the following steps to configure the application pool for ARCON SpectionUI.

1. Goto **Start** button and type **run**.
2. In **run** window type '**inetmgr**'. The **Internet Information Services (IIS) Manager** window opens.
3. Goto **Application Pool**.

4. Right-click on the Spection site.
5. The .NET CLR version should be set to **No Managed Code**.
6. Set Managed pipeline mode to **integrated**.
7. Right-click on spection on site list in IIS.
8. Add Application name- SpectionUI
9. Set **Alias: SpectionUI**.
10. Select ApplicationPool- **Spection**
11. Bind it pointing to SpectionUI folder.
12. Enable preload checkbox should be ticked.

Now we will Host Spection API as an application inside Spection site.

Use the following steps to add a new Spection API.

1. Right-click on the site on which SpectionUI is hosted.
2. Add application
3. Set **Alias: SpectionAPI**.
4. Select ApplicationPool- **Spection**
5. Bind it pointing to SpectionAPI folder.
6. Enable preload checkbox should be ticked.

2.4 Configurations

VideoLogs Configuration

To view the video logs perform the following steps.

- Right-click on the Spection site.
- Click Add application.
- Name of alias- SpectionVideo
- Bind it pointing to Arcos log archival folder(i.e. folder where LOB wise folder distribution exists)
- Enable directory browsing from IIS of that application

2.4.1 SpectionUI Configuration

- In the SpectionUI assets folder (\SpectionUI \assets), in file **config.json**, update the value parameter of "apiUrl" to the Url on which WebAPI will be hosted in IIS.
- (eg - http:ip:port/SpectionAPI)
- Edit sessionVideoUrl to http:ip:port/SpectionVideo
- Edit exportFolderUrl to http:ip:port/SpectionPdf
(name as mentioned while adding application on iis)

2.4.2 SpectionAPI Configuration

- In SpectionAPI's folder (\SpectionAPI), in **appsettings.json**, update the value parameter of "UiUrl" to the Url on which SpectionUI is hosted in IIS.
- (eg - http:ip:port/SpectionUI/)
- In SpectionAPI's folder (\SpectionAPI\DBSetting), open ARCOSDBSettingCreator.exe and generate dbsetting.ini.
- Edit fileurl to the above folder path
- Edit imagePath to the path of the default image in Images folder in SpectionApi package.
[any other image path can also be added in this place]

- edit watermark path to the path of the default watermark image in Images folder in SpectionApi package [any other watermark can also be added in this place]

2.4.3 ARCOSClientManagerOnline Configuration

- In the publish of ACMO → SAML folder → **samlSPEntities.json** → change the value of key: ConsumerServiceUrl and TargetUrl of **EntityCode:"PAMSPECTION"** to the Url on which the Spection API is hosted.
- ConsumerServiceUrl : <http://IP:port/SpectionAPI/api/SpectionAuth/Index2>
- TargetUrl : <http://IP:port>)

File Configuration

To generate reports in PDF format perform the following steps.

- Right-click on the Spection site.
- Click Add application.
- Name of alias- SpectionPdf
- Bind it to a folder(can be a new folder in Spection package)



- To run the scheduler, **ArconSpectionAlertService.msi** should be there in the package.
- Kindly set the value of **ApplicationUrl** as **SpectionApiUrl** in Program Files(x86)\ARCON Solutions\ArconSpectionAlertService\ArconSpectionSchedulerService.config. After installing the msi - Arcon Spection Alert Service should be visible in services.msc
- Check the chrome version of the application server on which SpectionApi is hosted.
- SpectionApi package contains ChromeDriver for version 90
- If any other version of chrome is present, then the ChromeDriver needs to be replaced in the package.

Access the application through Server Manager → Manager → My Apps → Spection



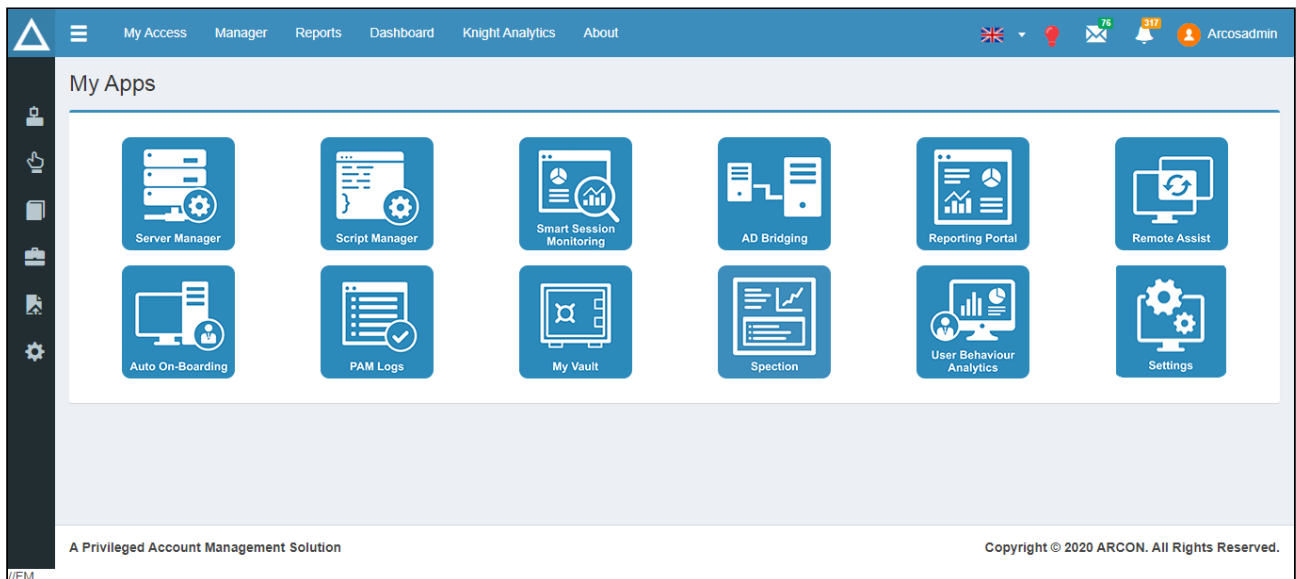
Only Administrators can assign the Spection privileges to the Users in the Server Manager. Once the privilege is assigned, Users can see the Spection tab in the Server Manager.

3 Accessing ARCON PAM Specion..

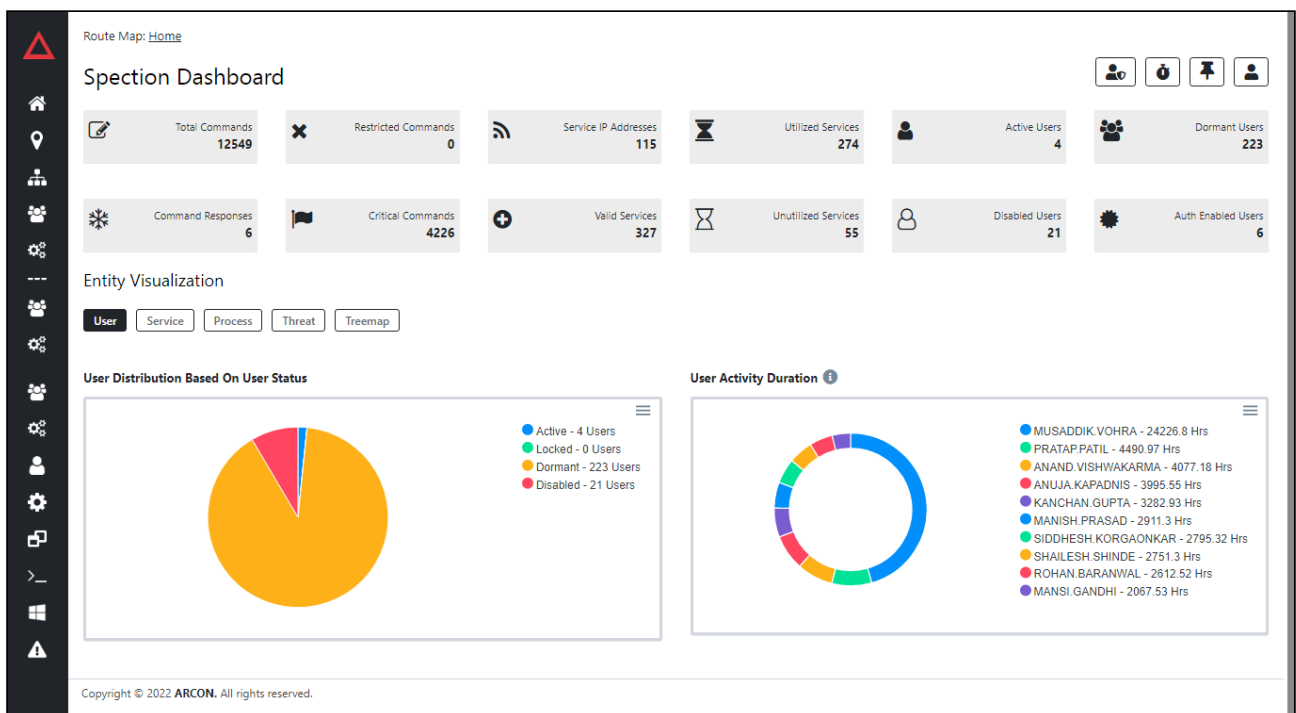
ARCON PAM Specion is present in the ARCON PAM Client Manager Online ACMO.

To navigate, use the following path:

Server Manager → Manager → My Apps → Specion



1. Click Specion App.
2. Specion will be opened in a new browser tab.



3.1 Specion Features

3.1.1 Entities of ARCON PAM


ARCON PAM Specion consists of the entities listed below. A basic understanding of these entities will give a comprehensive understanding of the reports.


Entities	Description
Site	This refers to the location of the office. Organizations can have offices in multiple locations. Users can generate different reports for different locations tagged under Site.
LOB	Line of Business (LOB). LOB can be very subjective depending on every organization. It can be different departments or teams within an organization. Technically there would be multiple user groups and service groups under each LOB. LOBs can be filtered based on <ul style="list-style-type: none">• LOB List: It will display the list of all the LOBs in ARCON PAM
User Group	This refers to the different user groups within the organization. User Group can be filtered based on <ul style="list-style-type: none">• User Group List: It will display the list of all the User Groups in ARCON PAM
Service Group	This refers to the different service groups in the organization. Service Group can be filtered based on <ul style="list-style-type: none">• Service Group List: It will display the list of all the Service Groups in ARCON PAM

Entities	Description
Users	<p>This refers to the list of individual users in the organization. Filters can be applied to the users on the basis of User list and User Properties.</p> <ul style="list-style-type: none"> • User List: It will display the list of all the individual users in ARCON PAM • User Properties: Users can be filtered on the basis of the features listed below. The available features are as follows: <ul style="list-style-type: none"> ▪ User Type: It will display the User Type which is Admin and Client. ▪ Domain: It will list all user domains in the organization ▪ Valid Until: It will allow users to select a date range, all users with the validity falling in the selected date range will be listed. ▪ Last Login: It will list all the users whose last login date falls under the selected date range. ▪ Authentication Enabled: The filter can be set to True or False, this is applicable only for those users who have the two-factor authentication enabled. ▪ Authentication Type: It will allow users to filter based on the different authentication methods in ARCON PAM. <ul style="list-style-type: none"> ◦ Biometric- Finger Print: It will allow users to filter all the users authenticated through Biometric Finger print. ◦ Email OTP: It will allow users to filter all the users authenticated through Email OTP. ◦ SMS OTP: It will allow users to filter all the users authenticated through SMS OTP. ◦ Mobile OTP: It will allow users to filter all the users authenticated through the configured Mobile OTP which is received on the ARCON Authenticator. ◦ Hardware Token: It will allow users to filter all the users authenticated through any Hardware token. ◦ Voice Biometric: It will allow users to filter all the users authenticated through voice biometric. ◦ User Door Access Authentication: It will allow users to filter all the users authenticated through User Door Access Authentication.
Services	<p>This refers to the list of individual services in the organization. Filters can be applied to the services based on the features listed below:</p> <ul style="list-style-type: none"> • Service Type: It will allow the users to set a filter based on different service types such as SybaseQA, MySQL QA, SSH Linux, Oracle QA, etc. • IP Address: It will list all the service IP Addresses available in ARCON PAM. • Port: It will list all the different service ports used in the ARCON PAM. • Instance: It will list all the instances present in the ARCON PAM. • Host: It will list all the available service host names in the ARCON PAM. • Username: It will list all the available service usernames in the ARCON PAM. • Domain: It will list all the service domain names available in the ARCON PAM. • Valid Until: Select a date range and it will list all the services whose validity expires/ expired during that period.
Sessions	<p>This refers to a specific instance of a user accessing a service through Arcon PAM. Filters can be applied to the sessions based on the features listed below:</p> <ul style="list-style-type: none"> • Session Started On: Select the session Start date from the date report should be generated. • Session Ended On: Select the session End date till the date report should be generated.

Entities	Description
Commands	<p>It is an instruction causing a computer or a server to perform one of its basic functions. Filters can be applied to the Commands based on the Command properties listed below:</p> <ul style="list-style-type: none"> • TimeStamp: Select the date range for which the report should be generated. • Response: Select the command response types from the Response list. For example: If a particular command is restricted/critical. • Critical: Select the type of critical commands i.e True or False which are to be included in the report.
Process	<p>A process is an instance of a program running on a computer. Filters can be applied to the Processes based on the process properties listed below:</p> <ul style="list-style-type: none"> • Process Timestamp: Select the date range for which the report should be generated. • Process Name: It will display the list of all the processes used in ARCON PAM. • Is Restricted: The filter can be set to True or False.
Threat	<p>The threat refers to the detailed list of outsiders (unauthorized users) trying to access the services. Filters can be applied to the Processes based on the process properties listed below:</p> <ul style="list-style-type: none"> • IP Address: It will list all the service IP Addresses available in ARCON PAM. • Username: It will list all the available service usernames in the ARCON PAM • Domain: It will list all the service domain names available in the ARCON PAM • Accessed On: Select the date range for the outside access report should be generated. • Action Performed: The user can filter the report based on the action type selected: <ul style="list-style-type: none"> ▪ Email Notification ▪ No Action

3.1.2 Privilege Based Access

The Privilege Based Access  feature is used by the Super Admin to manage user access on Spection. The Privilege Based Access icon will only appear to the Super Admin, who will have the access to all data in the Spection. To manage the privilege based access:

1. Click on the  icon present on the Dashboard.
2. The Privilege Based Access Report appears as shown in the screen below:

Privilege Based Access Report						
Show <input type="text" value="10"/> entries			Search: <input type="text" value="Press Enter to Search"/>			
Sr.No	User Name	Privilege Type	Privilege Assigned On	LOB Assigned	Modify	Delete
1	PARAGH SHAH	All Data	03/01/2022 19:06:20	-		
2	PRANAV BHATIA	LOB Based	07/12/2021 14:38:09	ARCON PAM,NEW_LOB		
3	USER3	LOB Based	12/10/2020 12:01:32	ARCON EXTERNAL,ARCON PAM,NEW_LOB		
4	USER2	LOB Based	12/10/2020 12:00:36	ARCON PAM,NEW_LOB,PIZZA_TEST,SP_TEST		
5	NEEL B	LOB Based	12/10/2020 11:55:49	ARCON PAM,SP_TEST		
6	J BUTLER	LOB Based	11/20/2020 15:55:01	ARCON EXTERNAL,ARCON PAM		
7	JOHN D	LOB Based	11/20/2020 15:54:33	ARCON EXTERNAL,ARCON PAM		
8	NILAY	LOB Based	11/20/2020 15:52:14	ARCON PAM		
9	NITESH P	LOB Based	08/26/2020 15:30:33	ARCON PAM		
10	TEST B	LOB Based	07/13/2020 11:16:19	ARCON EXTERNAL		
Showing 1 to 10 of 18 entries					Previous	1 2 Next
Copyright © 2022 ARCON. All rights reserved.						

Refer to the table below to understand the data displayed in the Privilege Based Access Report.

Column Name	Description
User Name	Specifies the name of the user.
Privilege Type	Specifies the type of privilege: <ul style="list-style-type: none"> LOB Based: The user can access the respective LOB assigned. All Data: The user can access all the data on Specion.
Privilege Assigned On	Specifies the date and time on which, the privilege was assigned.
LOB Assigned	If the user's privilege type is LOB Based , then the respective LOB assigned to the user will be displayed in this field. If the user's privilege type is All Data , then - will be displayed.
Modify	By clicking on the modify icon, the super admin will be able to modify the privileges of the respective user.
Delete	By clicking on the delete icon, the super admin will be able to delete the respective user.

Modifying the user privileges

Once the super admin clicks on the modify icon from the Privilege Based Access Report, the Privilege Based Access Configuration pop-up appears:



Privilege Based Access Configuration

Select User

Super Admin

Privilege Type

All Data

All Data

LOB Based

Modify

Based on the requirement, the Super Admin can update the Privilege Type field as All Data/LOB Based and click on **Modify** to save the changes.

3.1.3 Scheduling Report

Scheduling report means sending reports automatically to the configured users by email at specific time intervals. To Schedule a report



1. Click on the icon on Dashboard.
2. It directs to the scheduler master report page which lists all the schedulers.

3.1.3.1 Create a scheduler

Administrative users can configure the scheduler here.

Scheduler Master Report
Scheduler Configuration
SMTP Configuration

Scheduler Configuration

Schedule Name

user rep

Schedule Description

Start Time

07/01/2021 12:28

Expiry Time

06/30/2051 12:17

Weekly

Monthly

Yearly

☒ Monday
☒ Wednesday
☒ Friday
☐ Sunday

☒ Tuesday
☒ Thursday
☐ Saturday

at

12

:

33

To Email ID's (Enter ; between 2 email id's)

pranay.bhatia@arconnet.com;parakh.shah@arconnet.com;prachi.sanghvi@arconnet.com

Email Subject

user

Email Body

user

Export Type

Is Active

☒

Modify

Copyright © 2021 ARCON. All rights reserved.

The description of the fields are given below

Column Names	Description	
Schedule Name	The name of the scheduler	
Schedule Description	Text entered during the creation of scheduler	
Start Time	Date-time from which the scheduler should work	
Expiry Time	Date-time till which the scheduler should work	
Schedule	Schedule the report to run weekly, monthly or yearly	
	Weekly	Specify the days of the week and the time when the report will be generated.
	Monthly	Specify the day of the month, the frequency, and the time when the report will be generated.
	Yearly	Specify the month of the year, the frequency, and the time when the report will be generated.

Column Names	Description	
To Email IDs	Email IDs of the users who will receive reports automatically	
Email Subject	Subject of email	
Email Body	Body of email	
Export type	Format of report <ul style="list-style-type: none"> • CSV • PDF • XLSX 	
Is Active	If the scheduler should work	
Save	Saves the information	

3.1.3.2

View Configured scheduler

All the saved scheduler configurations are seen here.

Scheduler Master Report

Scheduler Configuration

SMTP Configuration

Scheduler Master Report

Show10entries

Add Scheduler

Search:

Sr.No	Scheduler Name	Scheduler Description	Scheduler Created On	Scheduler Type	Scheduler Information	Email Id(s)	Is Active	Modify	Delete
1	user rep		06/30/2021 12:17:59	weekly	At 12:33 PM, only on Monday, Tuesday, Wednesday, Thursday, and Friday	pranay.bhatia@arconnet.com	true		

Showing 1 to 1 of 1 entries

Previous1Next

Copyright © 2021 ARCON. All rights reserved.

3.1.3.3 SMTP Configuration

For scheduling, SMTP configuration is required. This is required to send emails to the configured users.

The screenshot displays the 'SMTP Configuration' window within the 'Scheduler Configuration' section. The window contains the following fields and controls:

- SMTP IP Address:** Text input field containing '10.10.0.23'.
- SMTP Port:** Text input field containing '25'.
- SMTP Email Id:** Text input field containing 'arcos.uat2@arconnet.com'.
- Display Name:** Text input field containing 'Arcon Spection'.
- SSL:** A toggle switch currently turned off.
- Update:** A button to save the configuration.

At the bottom of the application window, a copyright notice reads: 'Copyright © 2021 ARCON. All rights reserved.'

The description of the fields are given below

Column Names	Description
SMTP IP Address	The IP address of the SMTP server
SMTP Port	The port required to connect SMTP to the target server in order to send an email
SMTP Email ID	Email Id from which the user shall receive emails
Display Name	Display name of the sender
SSL	Enables SMTP on SSL
Save	Saves the information

3.1.4 Filtering

Filtering reports highlight the data of greater interest.

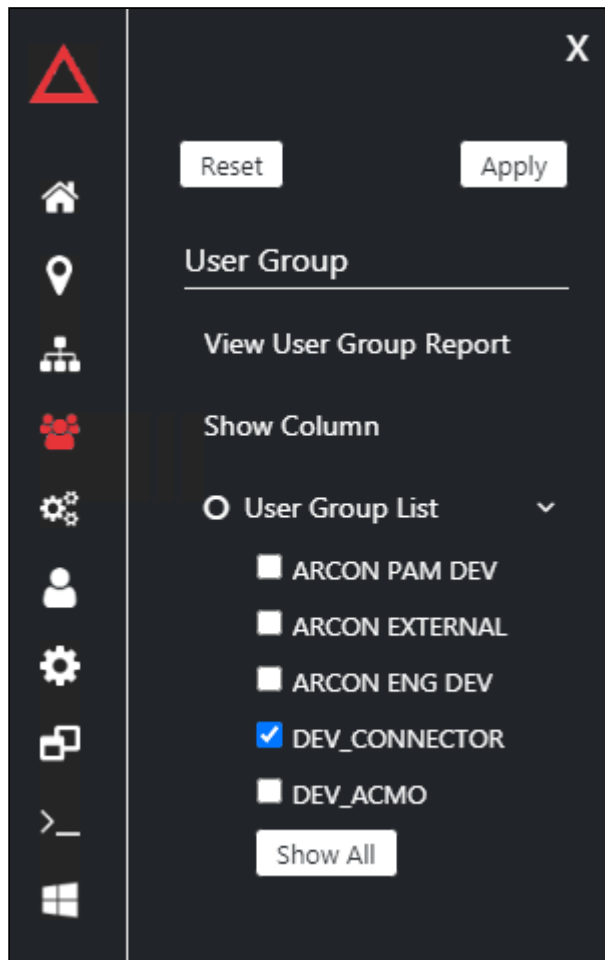
1. Complete Control

a. Filters

ARCON Spection filtering feature on the left pane limits the size of the report vertically.

b. Show/Hide Columns

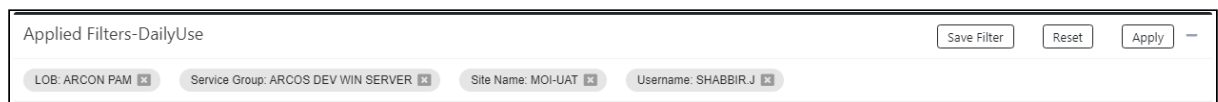
The Show column/ Hide column feature restricts the number of columns horizontally in a report thereby narrowing the areas of analysis.



2. Show Report

Once the filters are applied the users can jump to any report he wishes to. In this way, the need for selecting filters every time is eliminated.

3. Applied Filters



a. Save Filter

The save filter option saves your filter selection.

Save Filter As...

DailyUse

Save

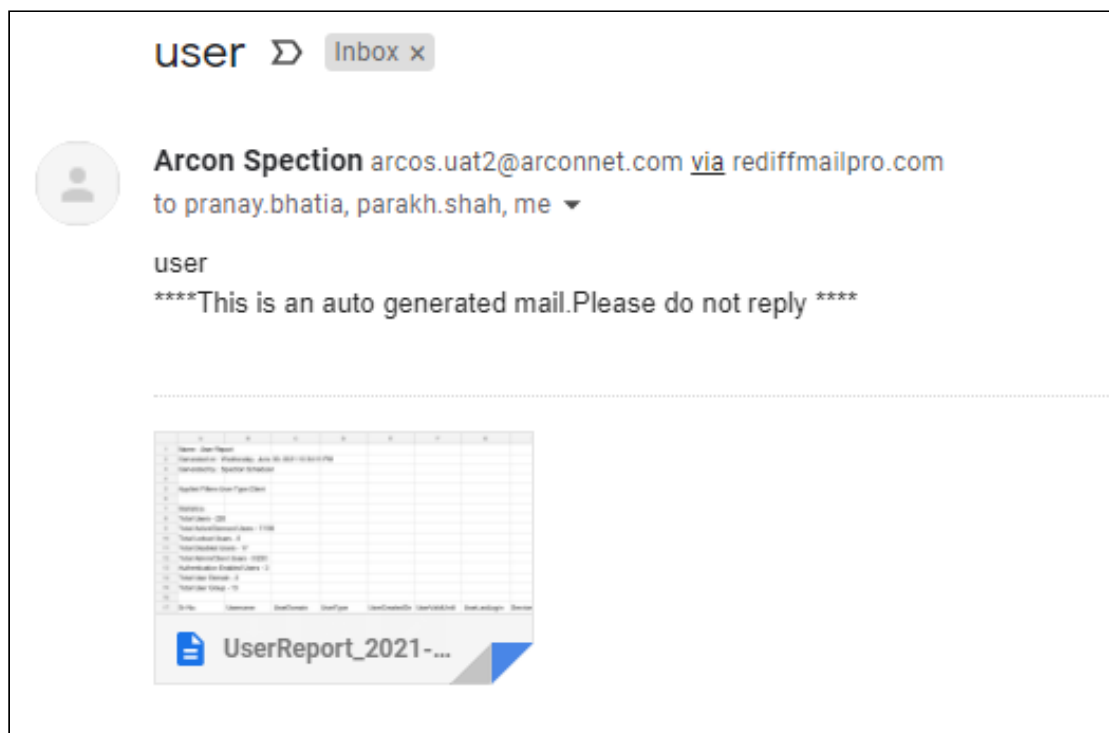
Cancel

b. Pinned Filter

The pinned filter enables to quickly filter the report without having to again choose the filters. It lands you directly to the report where it was pinned. A scheduler is assigned to the report from [here](#).

Pinned Filters ✕				
Filter Name	Filters	Report Name	Scheduler	View Delete
client	User Type:Client	User	user rep ▾	 

After assigning the scheduler to the report, the email is received.




c. **Reset**

The reset feature displays the default report without any filter.

d. **Apply**

Once the filters are selected, click the **Apply** button to see the changes. After the filter is applied, it can be **Removed** by selecting the close button on the top of the filter.

e. **Hide**

To **Hide** the filters, click on the  icon. Moreover, with the applied filters one can jump to different reports as well. The filters will change the statistics, graphs, and reports present on the dashboard.

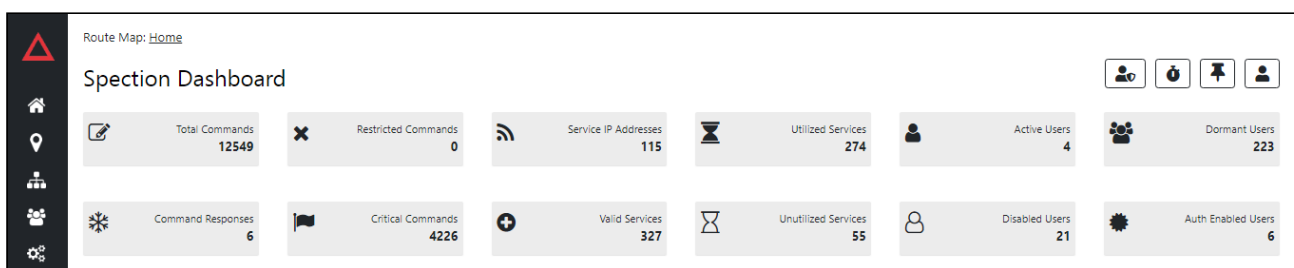
4 Spection Dashboard

A dashboard is a primary window through which you gain insights into your reporting data. The dashboard contains the following:

1. Widgets
2. Graphs
3. Access to all reports

4.1 Widgets

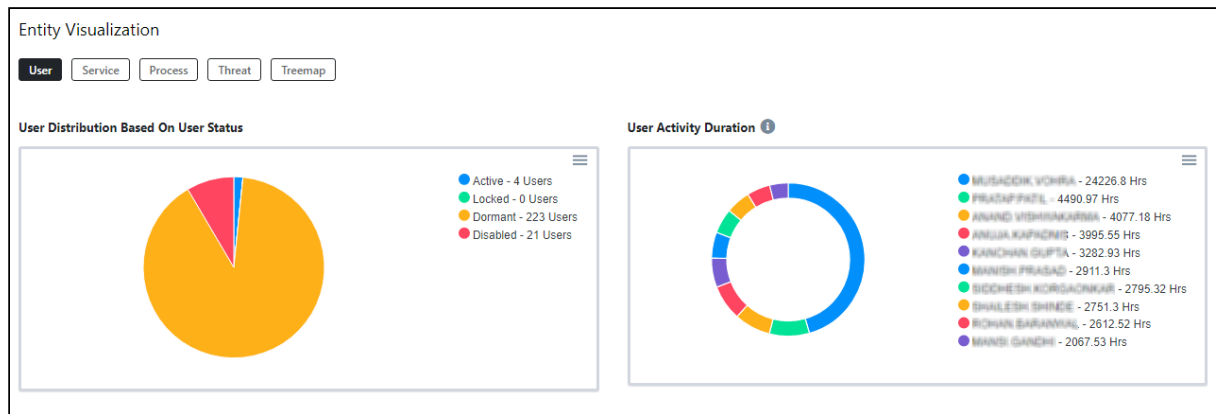
ARCON PAM Spection widgets display crucial information that is important to a user which makes them an essential aspect of home screen customization. They give us an "at-a-glance" view of the most important functionalities which is about the Users, Services, and Commands.



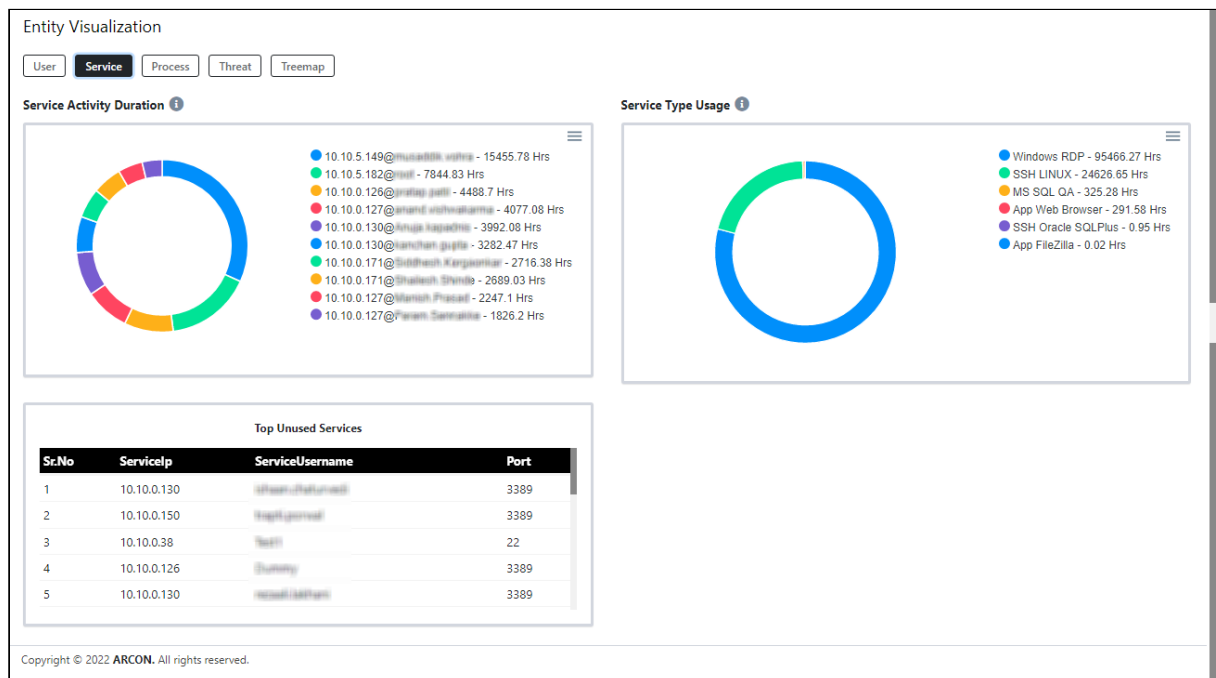
4.2 Graphs

It's a human tendency to look at an image first and text later. Graphical representation enhances the look and feel of the data. When you Look at numerical data it will not help in understanding the overall distribution of data but a graphical representation will give us more clarity and insight for the same. These graphs are dynamic and will change whenever the nodes or circles are clicked or the filters are applied. ARCON Spection Graphs are available in the following formats.

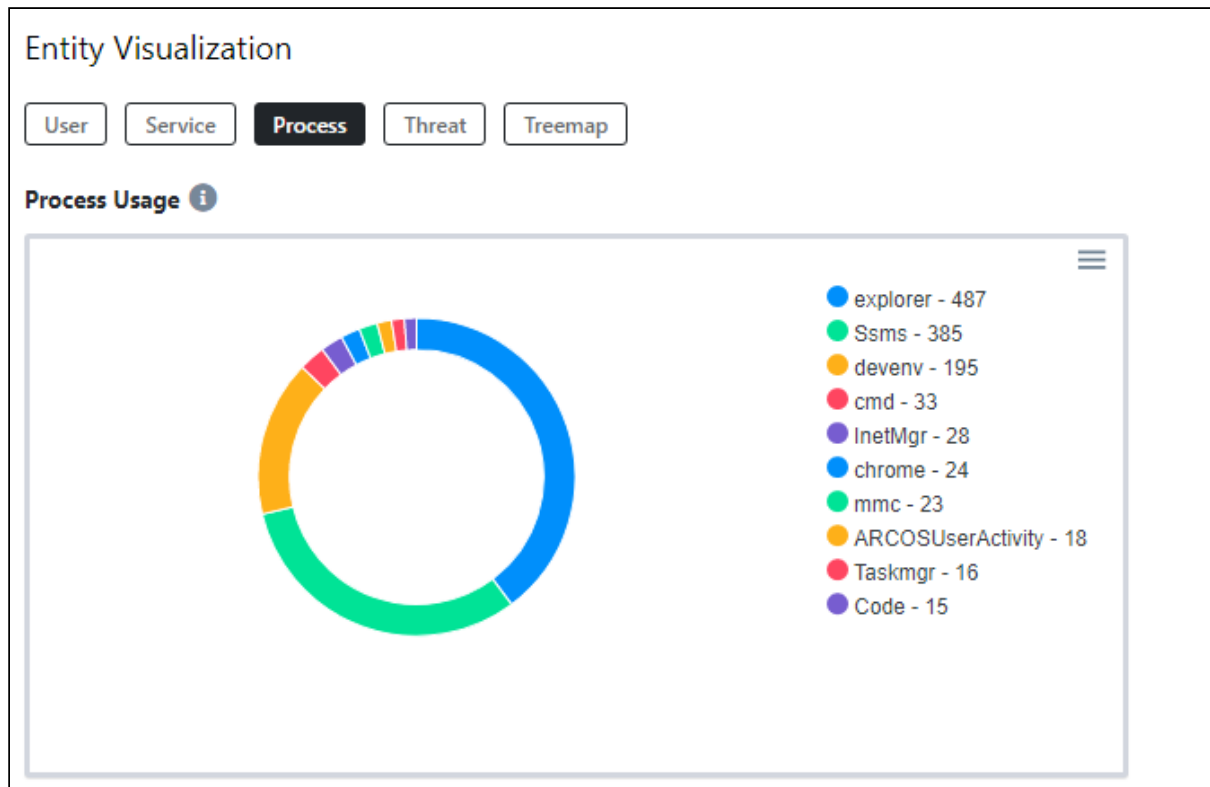
1. **Users-** The User entity contains two charts:
 - a) **User Distribution Based On User Status:** As the name suggests, the pie-chart represents the users distributed by the status such as Active, Locked, Dormant, and Disabled.
 - b) **User Activity Duration:** this chart represents the user activity distributed by the duration in hours (hrs).



2. **Service-** The Service entity contains two charts and one table:
- Service Activity Duration:** This chart represents the different service activities distributed by the time duration in hours.
 - Service Type Usage:** This chart represents the different service type usage time distributed in hours.
 - Top Unused Service:** As the name suggests, this table displays the data of top unused services along with service IP, service username, and the port number.



3. **Process-** The Process entity contains the **Process Usage** chart that represents all the different processes distributed by the usage in numbers.



4. **Threat:** The Threat entity contains two tables:
- Recent Outside Accessed Services:** This table displays the recently outside accessed services along with service name and the date & time of service accessed.
 - Most Outside Accessed Services:** This table displays the topmost outside accessed services along with the service name and the count.

Entity Visualization

User Service Process **Threat** Treemap

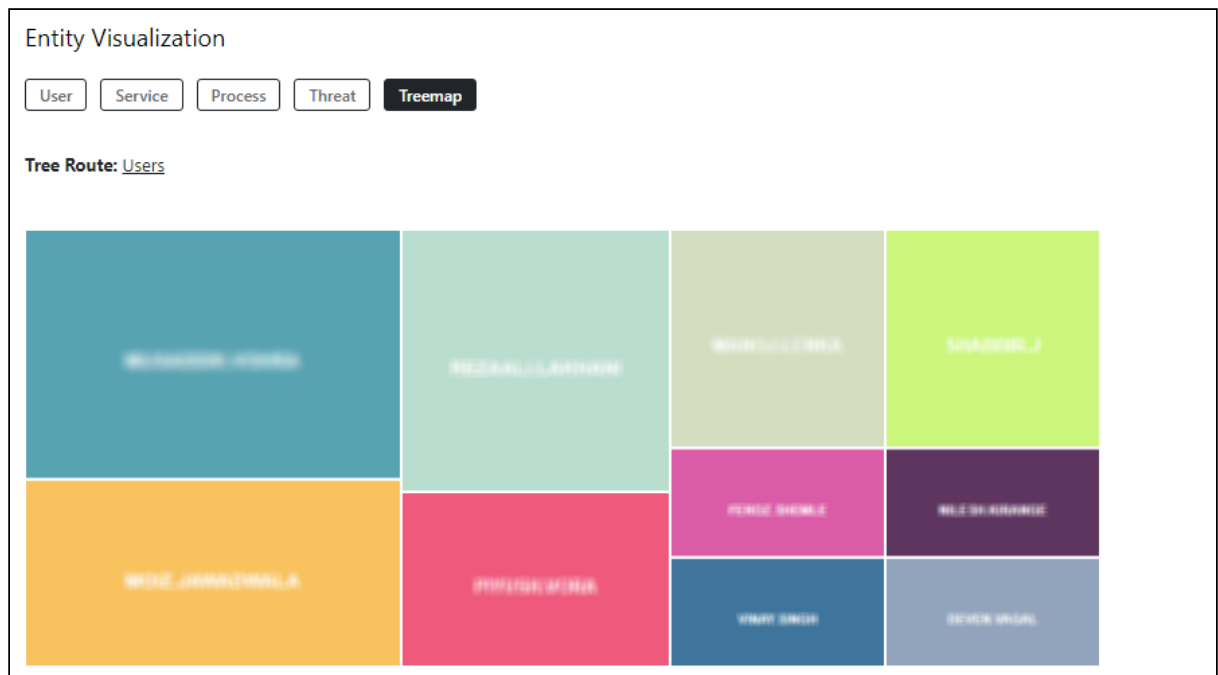
Recent Outside Accessed Services i

Service	Service Accessed On
10.10.0.176@Administrator	08/23/2021 12:09:52
10.10.0.176@PranayBhatia	02/01/2021 15:24:22
10.10.0.176@PranayBhatia	02/01/2021 15:23:58
10.10.0.176@PranayBhatia	02/01/2021 15:23:36
10.10.0.176@ParakhShah	02/01/2021 15:22:15

Most Outside Accessed Services i

Service	Count
10.10.0.176@ParakhShah	353
10.10.0.176@PranayBhatia	266
10.127.127.1@ParakhShah	185
10.127.127.1@PranayBhatia	141
10.10.0.91@vishant.verma	11

5. **Treemap:** The Treemap entity consists of different tiles that represents the username. By clicking on the user tile, the services that have been assigned to the respective user will appear. By clicking on the service tile, the commands that have been fired for that respective service will appear.



4.3 Access to all reports

All the reports can be accessed by clicking the report button which is below the widgets and above the graphs. The following reports are available:

1. LOB Report
2. User Group Report
3. Service Group Report
4. User Report
5. Service Report
6. Session Report
7. Command Report
8. Process Report
9. Outside Arcos Access/Threat Report

A detailed reporting functionality is explained under the Reports Walkthrough section.

5 Spection Reports

5.1 LOB Report

LOB Report is a report which displays details of all the LOBs created in ARCON PAM. LOB reports help to generate a graphical view and exact count of individual, and groupwise details of users and services. It further displays details such as LOB name, who has created the LOB, and when the LOB was created. Before we walk through the LOB report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**-It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**-The searching filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**-The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV, and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.1.1 LOB Report Generation

Let us generate the LOB Report to see the number of admins who didn't fire any critical commands in each LOB.

We need to apply the following filters:- User Type = Admin, and Critical Command = False.



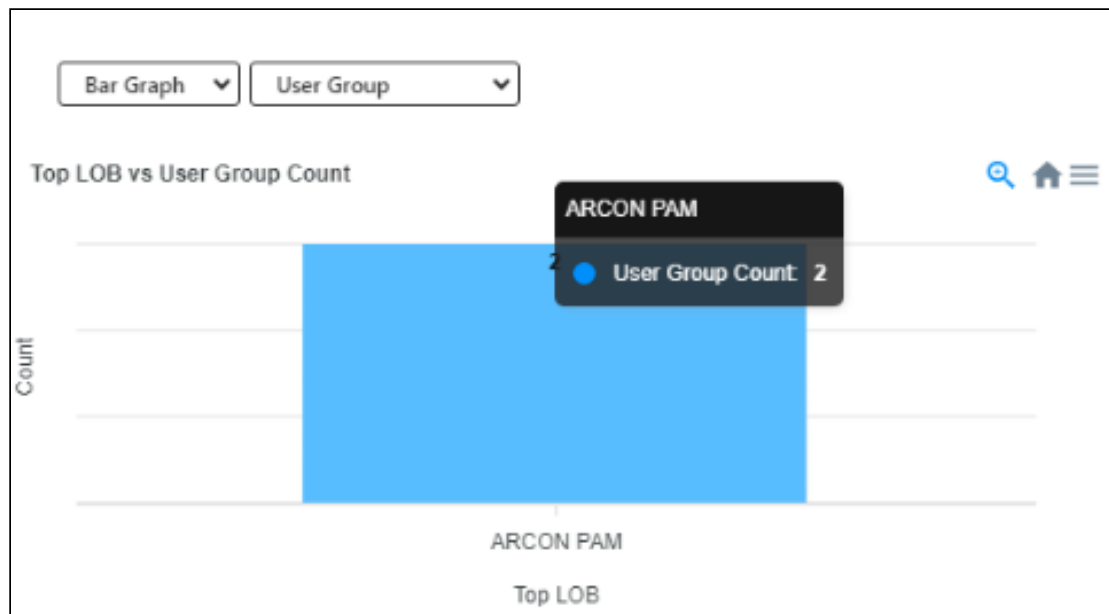
The LOB report consists of 3 major sections which are described below.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. LOB Report statistics summary is displayed below.

LOB Report	
Total LOB	1
Total User Group	1
Total Service Group	2
Total Users	4
Total Services	4
Total Sessions	21
Total Commands	60
Total Processes	0

2. **Graphs** :- Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are clickable and expand on selection.

- a. Bar Graph- It displays the data and the count of the selected item from the dropdown i.e from User Group-Service Group, Users-Services, Sessions, Commands, Critical Commands, and Processes in the graphical format. Graphs can be zoomed in by clicking. Additionally, the graphs can be downloaded in **SVG, PNG, and CSV** format.



3. **Report table**:- The tabular report displays the records in a grid format.

Applied Filters

Save Filter

Reset

Apply

Command Critical: False

User Type: Admin

Show10entries

Search: Press Enter to Search

Sr No.	LOB Name	LOB Created By	LOB Created On	User Group Count	Service Group Count	User Count	Admin Count	Service Count	Session Count	Command Count	Command Critical Count	Process Count
1	ARCON PAM		01/16/2019 19:27:06	1	2	4	1	4	21	60	0	0

Showing 1 to 1 of 1 entries (filtered from 13 total entries)

Previous1Next

Copyright © 2022 ARCON. All rights reserved.

5.2 User Group Report

User Group Report is a report which displays details of all the user groups created in ARCON PAM. It displays details such as the name of the user group, the name of the user who has created the user group, and the date & time on which the user group is created. Before we walk through the User Group report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

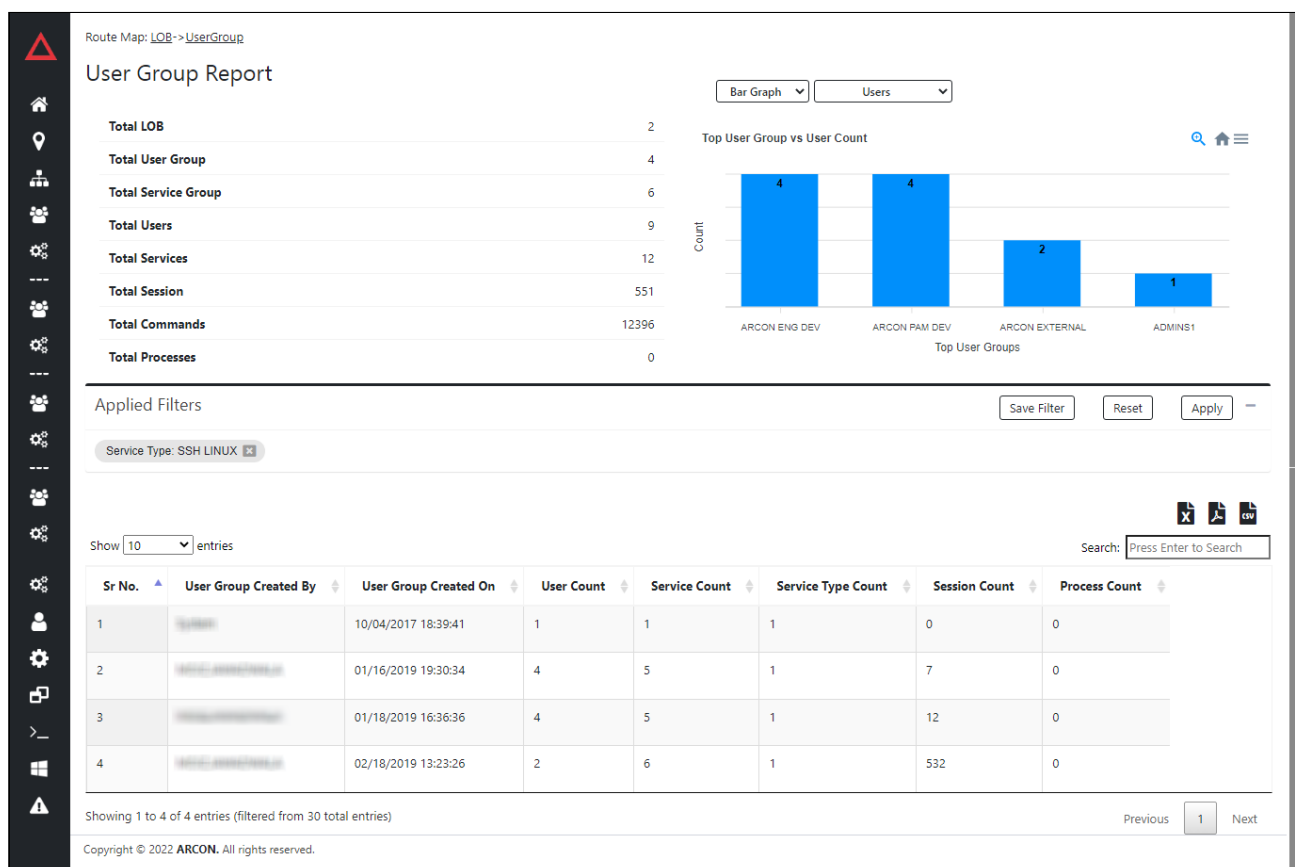
Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**- It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**-The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**- The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.2.1 User Group Report Generation

Let us generate the User Group report to see the number of users using SSH Linux services in each User group

We need to apply the following filters:- Service Type = SSH Linux, User-> Show Column, Command->Show Column.



The User Group report consists of 3 major sections which are described below.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. User Group Report statistic summary is displayed below.

User Group Report	
Total LOB	2
Total User Group	4
Total Service Group	6
Total Users	10
Total Services	12
Total Session	554
Total Commands	12425
Total Processes	0

2. **Graphs** :- Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are clickable and expand on selection.
 - a. Bar Graph- It displays the data and the count of the selected item from the dropdown i.e from User, User Type, User Domain, User Auth Enabled, Active Users, Sessions, Commands, and Critical Commands, and Processes in the graphical format. Graphs can be zoomed in by clicking. Additionally, the graphs can be downloaded in **SVG, PNG, and CSV** format.



3. Report table:- The tabular report displays the record in a grid format.

Applied Filters

Save Filter Reset Apply

Service Type: SSH LINUX

Show 10 entries

Search: Press Enter to Search

Sr No.	User Group Created By	User Group Created On	User Count	Service Count	Service Type Count	Session Count	Process Count
1		10/04/2017 18:39:41	1	1	1	0	0
2		01/16/2019 19:30:34	4	5	1	7	0
3		01/18/2019 16:36:36	4	5	1	12	0
4		02/18/2019 13:23:26	2	6	1	532	0

Showing 1 to 4 of 4 entries (filtered from 30 total entries)

Previous 1 Next

Copyright © 2022 ARCON. All rights reserved.

5.3 Service Group Report

Service Group Report is a report which displays details of all the service groups created in ARCON PAM. It displays details such as the name of the service group, name of the user who has created the service group, and the date & time on which the service group has been created. Before we walk through the Service Group Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**- It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**- The searching filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**- The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.3.1 Service Group Report Generation

Let us generate the Service Group report to see the number of services used by admins in each service group

We need to apply the following filters:- User Type = Admin, Service-> Show Column.

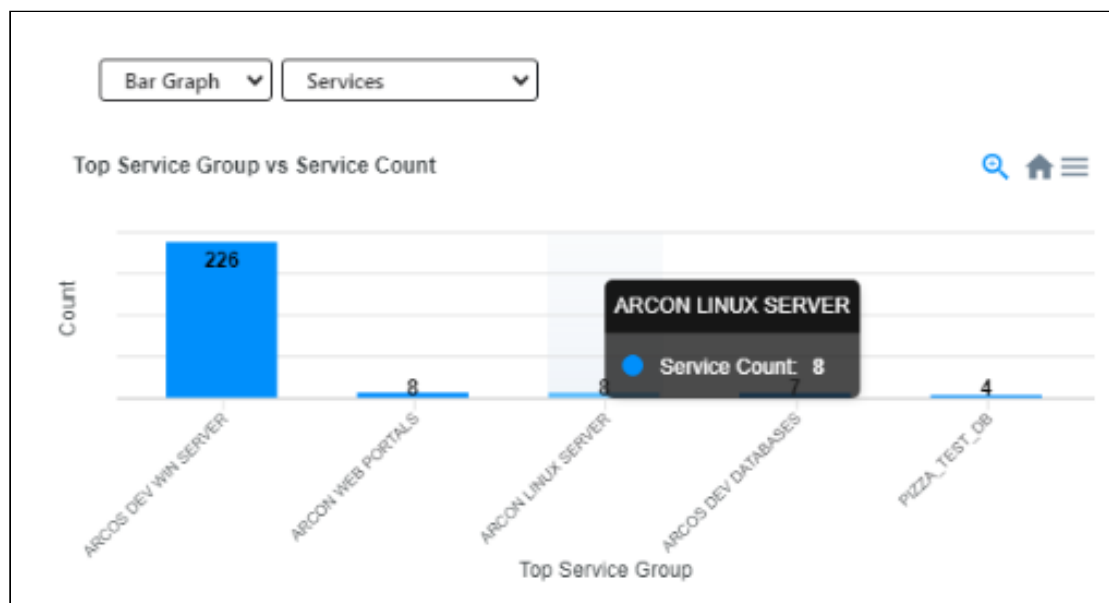


The Service Group report consists of 3 major sections which are described below.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. Service Group Report statistic summary is displayed below.

Service Group Report	
Total LOB	2
Total User Group	4
Total Service Group	6
Total Users	9
Total Services	12
Total Session	551
Total Commands	12396
Total Processes	0

2. **Graphs** :- Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are clickable and expand on selection.
 - a. Bar Graph- It displays the data and the count of the selected item from the dropdown i.e from User, User Type, User Domain, User Auth Enabled, Active Users, Sessions, Commands, and Critical Commands, and Processes in the graphical format. Graphs can be zoomed in by clicking. Additionally, the graphs can be downloaded in **SVG, PNG, and CSV** format.



3. **Report table**:- The tabular report displays the record in a grid format.

Applied Filters										
<div> <div>Save Filter</div> <div>Reset</div> <div>Apply</div> </div>										
<div> <div>Show 10 entries</div> <div>Search: <input type="text" value="Press Enter to Search"/></div> </div>										
Sr No.	Service Group Name	Service Group Created By	Service Group Created On	User Count	Admin Count	Service Count	Service Type Count	Session Count	Command Count	Process Count
1	ARCOS DEV WIN SERVER		01/16/2019 19:32:41	3	1	1	1	0	0	0
2	ARCOS DEV DATABASES		01/17/2019 09:34:54	3	1	1	1	0	0	0
3	ARCON LINUX SERVER		01/17/2019 09:35:23	7	1	5	1	19	225	0
4	SERVER EXTERNAL		02/18/2019 18:48:18	2	0	6	1	532	12171	0
5	MUM PAM SG		05/24/2021 16:56:46	0	0	1	1	0	0	0
6	DEL PAM SG		05/24/2021 16:57:26	0	0	5	1	0	0	0
<div> <div>Showing 1 to 6 of 6 entries (filtered from 32 total entries)</div> <div> <div>Previous</div> <div>1</div> <div>Next</div> </div> </div>										
Copyright © 2022 ARCON. All rights reserved.										

5.4 User Report

User Report is a report which displays details related to users whether they are active, inactive, which domain the user belongs to, users validity, LOB, and Groups the user belongs to in ARCON PAM. Before we walk through the User Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

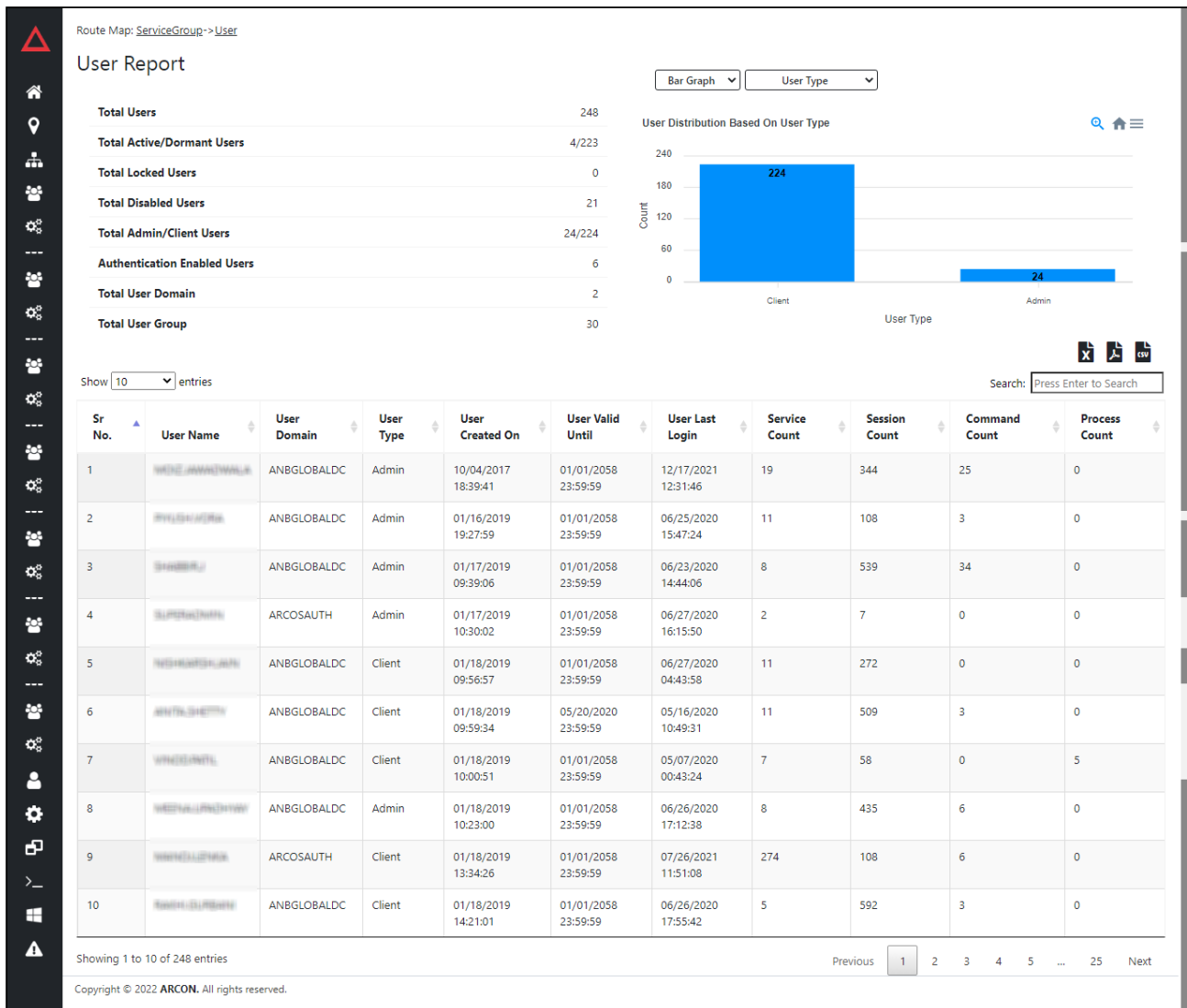
Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**- It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**- The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**- The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.4.1 User Report Generation

Let us generate the User report to see a list of users who have fired critical commands.

We need to apply the following filters:- Critical Commands = True.

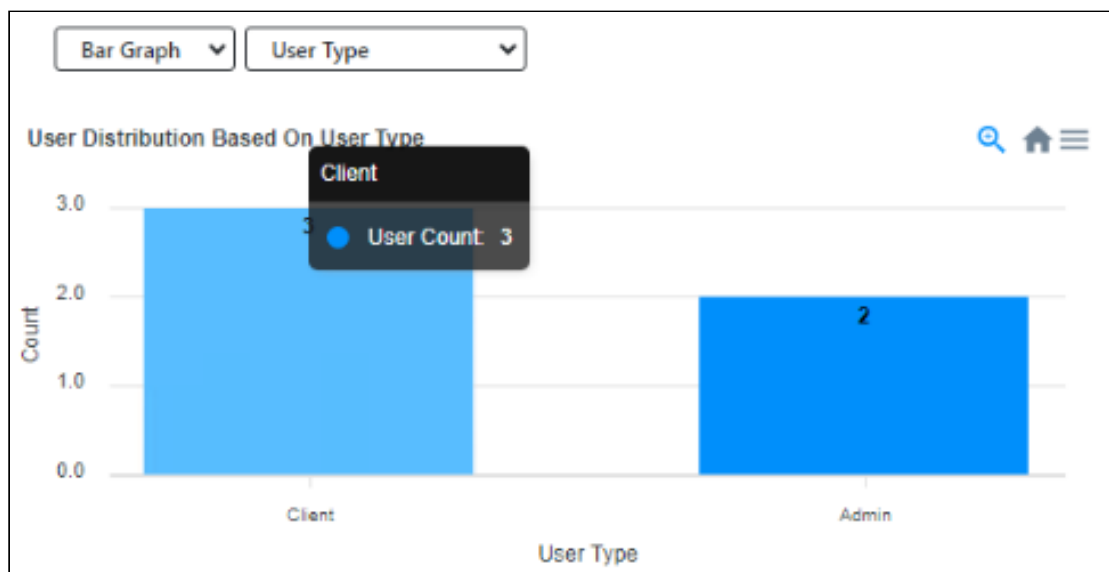


The User Report consists of 3 major sections which are described below.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. User Report statistic summary is displayed below.

User Report	
Total Users	5
Total Active/Dormant Users	0/5
Total Locked Users	0
Total Disabled Users	0
Total Admin/Client Users	2/3
Authentication Enabled Users	0
Total User Domain	2
Total User Group	3

2. **Graphs** :- Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are clickable and expand on selection.
 - a. **Bar Graph**- It displays the data and the count of the selected item from the dropdown i.e from Users, User Type, User Domain, User Authentication Enabled, Active Users, Sessions, Commands, Critical commands, and Processes in pictorial format. Graphs can be zoomed in by clicking. Additionally, the graphs can be downloaded in **SVG, PNG, and CSV** format.



3. **Report table**:- The tabular report displays the record in a grid format.

Show entries

Search:

Sr No.	User Name	User Domain	User Type	User Created On	User Valid Until	User Last Login	Service Count	Session Count	Command Count	Process Count
1	ADMINISTRATOR	ANBGLOBALDC	Admin	10/04/2017 18:39:41	01/01/2058 23:59:59	12/17/2021 12:31:46	19	344	25	0
2	SYSTEM	ANBGLOBALDC	Admin	01/16/2019 19:27:59	01/01/2058 23:59:59	06/25/2020 15:47:24	11	108	3	0
3	ADMINISTRATOR	ANBGLOBALDC	Admin	01/17/2019 09:39:06	01/01/2058 23:59:59	06/23/2020 14:44:06	8	539	34	0
4	ADMINISTRATOR	ARCOSAUTH	Admin	01/17/2019 10:30:02	01/01/2058 23:59:59	06/27/2020 16:15:50	2	7	0	0
5	ADMINISTRATOR	ANBGLOBALDC	Client	01/18/2019 09:56:57	01/01/2058 23:59:59	06/27/2020 04:43:58	11	272	0	0
6	ADMINISTRATOR	ANBGLOBALDC	Client	01/18/2019 09:59:34	05/20/2020 23:59:59	05/16/2020 10:49:31	11	509	3	0
7	ADMINISTRATOR	ANBGLOBALDC	Client	01/18/2019 10:00:51	01/01/2058 23:59:59	05/07/2020 00:43:24	7	58	0	5
8	ADMINISTRATOR	ANBGLOBALDC	Admin	01/18/2019 10:23:00	01/01/2058 23:59:59	06/26/2020 17:12:38	8	435	6	0
9	ADMINISTRATOR	ARCOSAUTH	Client	01/18/2019 13:34:26	01/01/2058 23:59:59	07/26/2021 11:51:08	274	108	6	0
10	ADMINISTRATOR	ANBGLOBALDC	Client	01/18/2019 14:21:01	01/01/2058 23:59:59	06/26/2020 17:55:42	5	592	3	0

Showing 1 to 10 of 248 entries

Previous **1** 2 3 4 5 ... 25 Next

Copyright © 2022 ARCON. All rights reserved.

5.5 Service Report

A service is an instance of a server. Each user may have a unique requirement of service to perform on the server. Service Report is used to generate details of services, which are active in ARCON PAM. In addition, it generates details of service type, domain, and instance of services. Before we walk through the Service Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

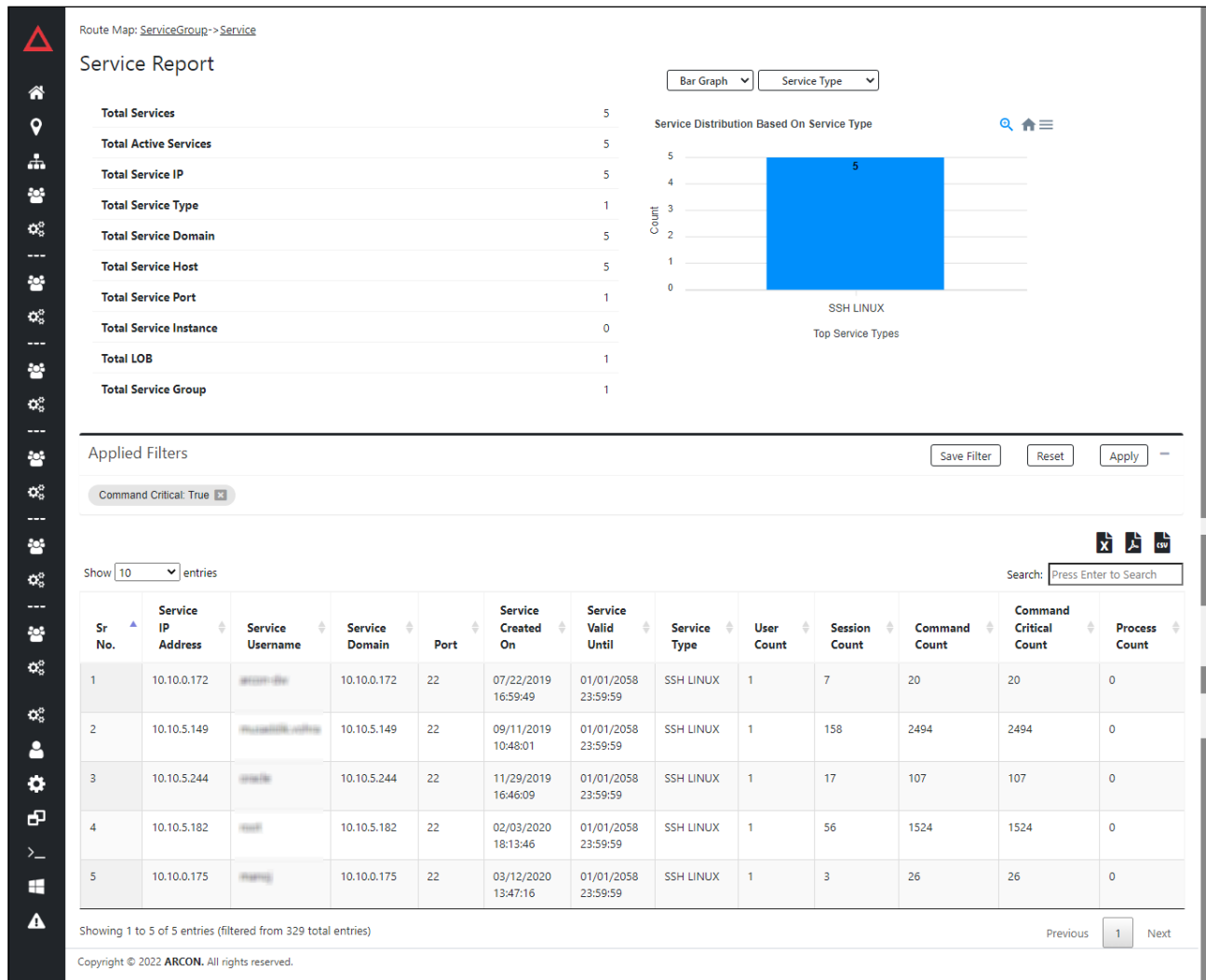
Report builder Functionalities

- **Apply/Reset filter-** Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter-** The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries-** It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching-** The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting-** The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination-** The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF-** All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo-** To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.5.1 Service Report Generation

Let us generate the Service report to see a list of service IPs and their service type, where most critical commands have been fired, and by number of users

We need to apply the following filters:- Critical command = True, Service Type -> Show Column, Users -> Show Column, and sort by critical commands



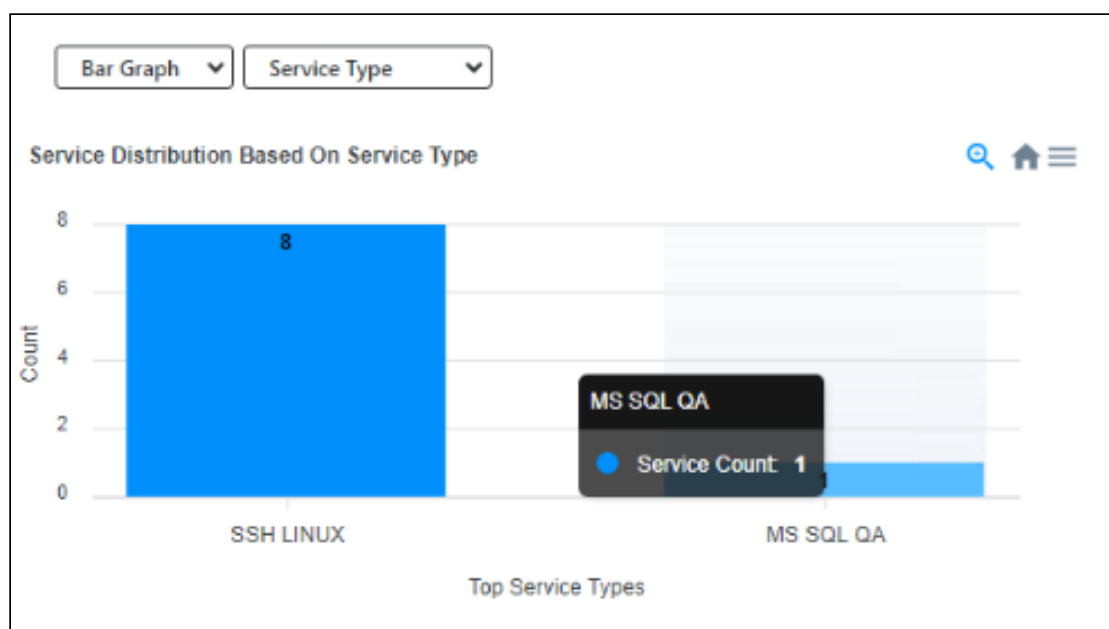
The Service Report consists of 3 major sections which are described below.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. Service Report statistic summary is displayed below.

Service Report

Total Services	9
Total Active Services	9
Total Service IP	8
Total Service Type	2
Total Service Domain	8
Total Service Host	8
Total Service Port	2
Total Service Instance	1
Total LOB	2
Total Service Group	4

2. **Graphs** :- Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are clickable and expand on selection.
- a. **Bar Graph**- It displays the data and the count of the selected item from the dropdown i.e from Service Type, Top 5 Service IPs, and Service Instance in the graphical format. Graphs can be zoomed in by clicking. Additionally, the graphs can be downloaded in **SVG, PNG, and CSV** format.



3. Report table:- The tabular report displays the record in a grid format.

Applied Filters

Save Filter
Reset
Apply

Command Critical: True

Show
10
entries

Search:
Press Enter to Search

Sr No.	Service IP Address	Service Username	Service Domain	Port	Service Created On	Service Valid Until	Service Type	User Count	Session Count	Command Count	Command Critical Count	Process Count
1	10.10.0.172	arcon-001	10.10.0.172	22	07/22/2019 16:59:49	01/01/2058 23:59:59	SSH LINUX	1	7	20	20	0
2	10.10.5.149	arcon-001	10.10.5.149	22	09/11/2019 10:48:01	01/01/2058 23:59:59	SSH LINUX	1	158	2494	2494	0
3	10.10.5.244	arcon-001	10.10.5.244	22	11/29/2019 16:46:09	01/01/2058 23:59:59	SSH LINUX	1	17	107	107	0
4	10.10.5.182	arcon-001	10.10.5.182	22	02/03/2020 18:13:46	01/01/2058 23:59:59	SSH LINUX	1	56	1524	1524	0
5	10.10.0.175	arcon-001	10.10.0.175	22	03/12/2020 13:47:16	01/01/2058 23:59:59	SSH LINUX	1	3	26	26	0

Showing 1 to 5 of 5 entries (filtered from 329 total entries)

Previous
1
Next

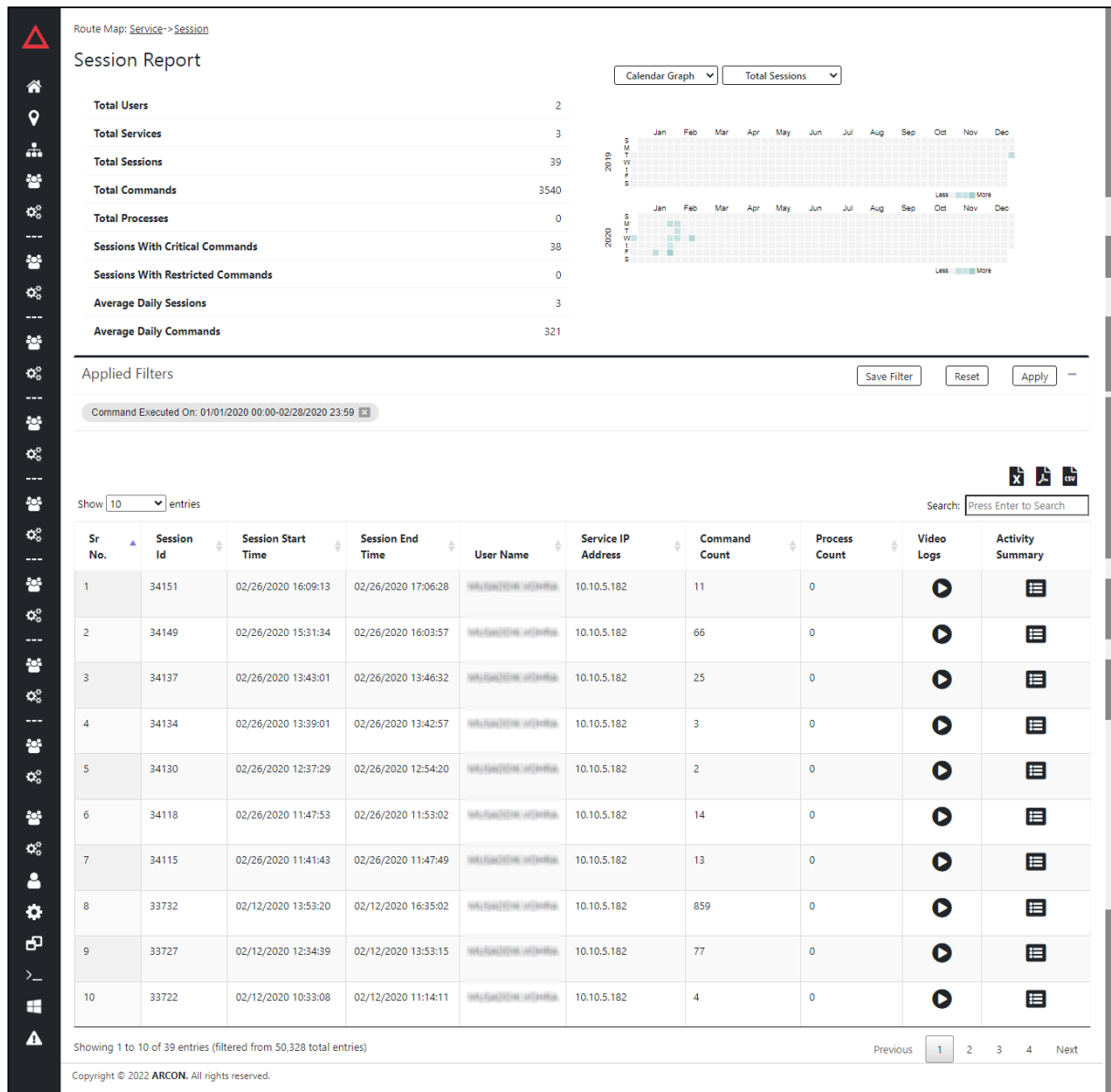
Copyright © 2022 ARCON. All rights reserved.

5.6 Session Report

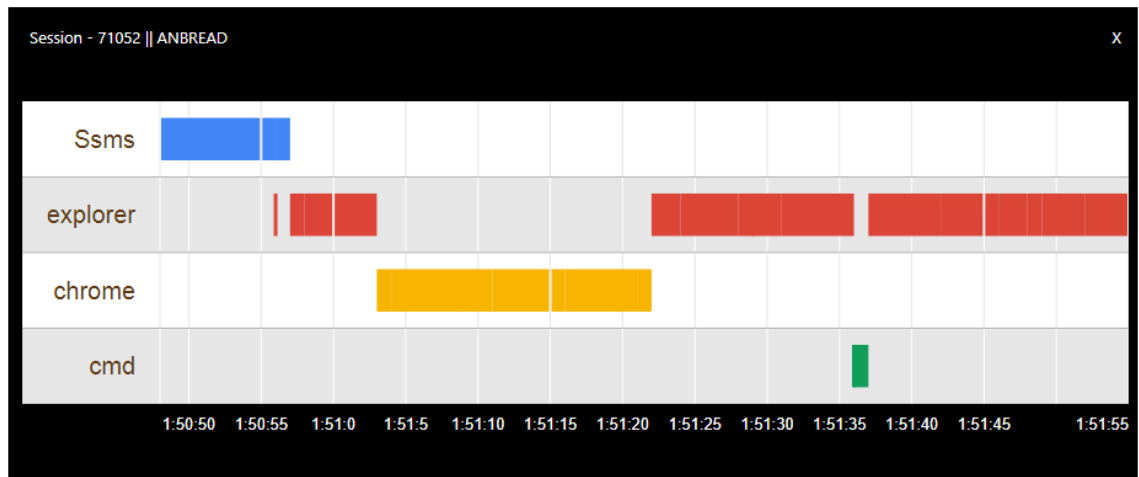
Session Report displays session-wise count of activities performed on Server along with details of service. It displays details such as session ID, start date and time of the session, end date and time of the session, User name, IP address of the server, count of critical commands executed in the session, count of restricted commands executed in the session, response count, and User group it belongs to. Before we walk through the Session Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Specion.

Features

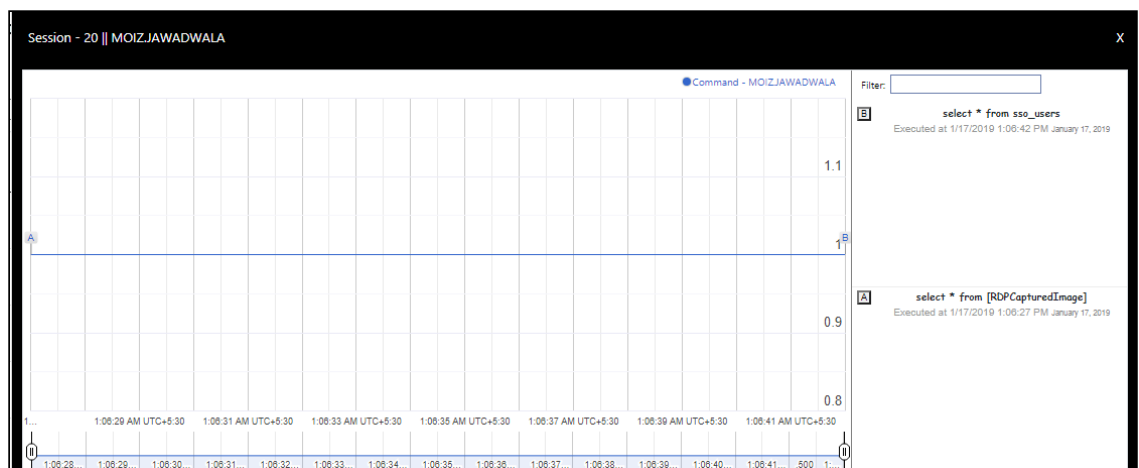
- Video Logs- Video logs are captured for each session. At a time 4 video logs can be played.



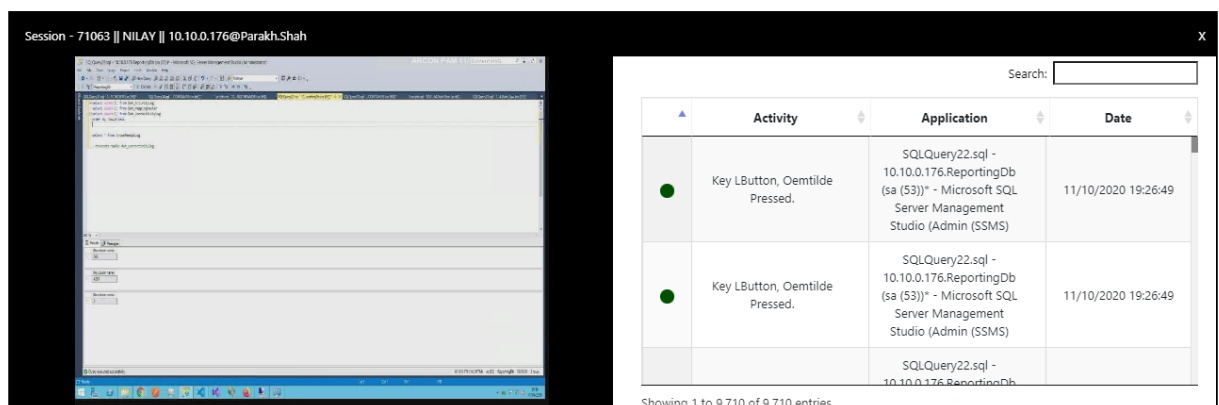
- Activity summary-
 - Activity summary of Windows services gives you the highlight of processes in each session for the given date-time range.




- Activity summary of Linux services gives you the highlight of commands fired in each session for the given date-time range.



- Smart Session Monitoring- It helps to monitor activities performed on Windows Server. One can view sessions of all users or specific users and session types they are running.



 To enable the Smart Session Monitoring feature, Smart session monitoring profile should be configured on ACMO.

Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**- It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**-The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**- The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.6.1 Session Report Generation

Let us generate the Session report to see a list of sessions taken last week and their associated user & service groups.

We need to apply the following filters:- Command Executed = Date range 01/01/2020-02/28/2020, User Group-> Show Column, Service Group->Show Column

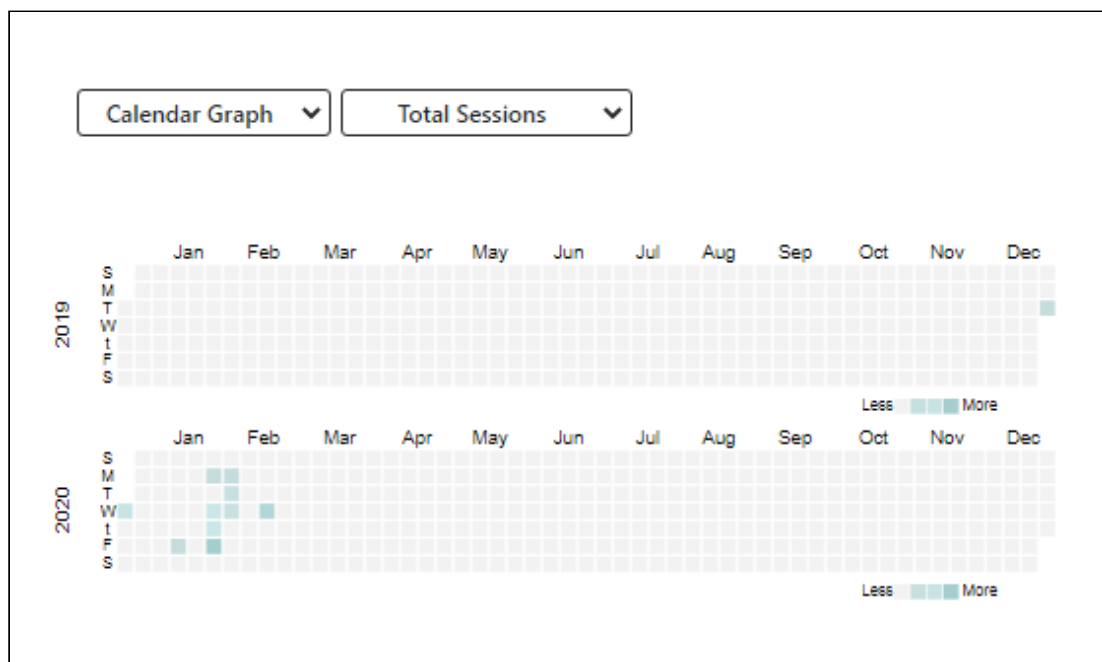
Applied Filters									
Command Executed On: 01/01/2020 00:00-02/28/2020 23:59									
<div> <div>Save Filter</div> <div>Reset</div> <div>Apply</div> </div>									
<div> <div> <div> <div> <div></div> <div></div> <div></div> </div> <div> <div></div> <div></div> <div></div> </div> </div> </div> </div>									
<div> <div> <div>Show</div> <div>10</div> <div>entries</div> </div> <div> <div>Search:</div> <div>Press Enter to Search</div> </div> </div>									
Sr No.	Session Id	Session Start Time	Session End Time	User Name	Service IP Address	Command Count	Process Count	Video Logs	Activity Summary
1	34151	02/26/2020 16:09:13	02/26/2020 17:06:28	...	10.10.5.182	11	0		
2	34149	02/26/2020 15:31:34	02/26/2020 16:03:57	...	10.10.5.182	66	0		
3	34137	02/26/2020 13:43:01	02/26/2020 13:46:32	...	10.10.5.182	25	0		
4	34134	02/26/2020 13:39:01	02/26/2020 13:42:57	...	10.10.5.182	3	0		
5	34130	02/26/2020 12:37:29	02/26/2020 12:54:20	...	10.10.5.182	2	0		
6	34118	02/26/2020 11:47:53	02/26/2020 11:53:02	...	10.10.5.182	14	0		
7	34115	02/26/2020 11:41:43	02/26/2020 11:47:49	...	10.10.5.182	13	0		
8	33732	02/12/2020 13:53:20	02/12/2020 16:35:02	...	10.10.5.182	859	0		
9	33727	02/12/2020 12:34:39	02/12/2020 13:53:15	...	10.10.5.182	77	0		
10	33722	02/12/2020 10:33:08	02/12/2020 11:14:11	...	10.10.5.182	4	0		
<div> <div>Showing 1 to 10 of 39 entries (filtered from 50,328 total entries)</div> <div> <div>Previous</div> <div>1</div> <div>2</div> <div>3</div> <div>4</div> <div>Next</div> </div> </div>									
Copyright © 2022 ARCON. All rights reserved.									

The Session Report consists of 3 major sections which are described below.

- 1. Statistics :-** Statistics give us an accurate count of the number of different attributes present. Session Report statistic summary is displayed below.

Session Report	
Total Users	2
Total Services	3
Total Sessions	39
Total Commands	3540
Total Processes	0
Sessions With Critical Commands	38
Sessions With Restricted Commands	0
Average Daily Sessions	3
Average Daily Commands	321

2. **Graphs :-** Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The Calendar graph displays the duration of the session based on the start time and the end time on the server. Filters can be applied on the session type i.e from Total sessions, Critical sessions, and Restricted sessions. The dark box displays higher session usage and light color indicates less sessions usage on that day.



3. **Report table:-** The tabular report displays the record in a grid format. Video logs, activity summary, and smart session monitoring of sessions can be viewed here.

Applied Filters

Save Filter

Reset

Apply

Command Executed On: 01/01/2020 00:00-02/28/2020 23:59

Show 10 entries

Search: Press Enter to Search

Sr No.	Session Id	Session Start Time	Session End Time	User Name	Service IP Address	Command Count	Process Count	Video Logs	Activity Summary
1	34151	02/26/2020 16:09:13	02/26/2020 17:06:28	...	10.10.5.182	11	0	▶	☰
2	34149	02/26/2020 15:31:34	02/26/2020 16:03:57	...	10.10.5.182	66	0	▶	☰
3	34137	02/26/2020 13:43:01	02/26/2020 13:46:32	...	10.10.5.182	25	0	▶	☰
4	34134	02/26/2020 13:39:01	02/26/2020 13:42:57	...	10.10.5.182	3	0	▶	☰
5	34130	02/26/2020 12:37:29	02/26/2020 12:54:20	...	10.10.5.182	2	0	▶	☰
6	34118	02/26/2020 11:47:53	02/26/2020 11:53:02	...	10.10.5.182	14	0	▶	☰
7	34115	02/26/2020 11:41:43	02/26/2020 11:47:49	...	10.10.5.182	13	0	▶	☰
8	33732	02/12/2020 13:53:20	02/12/2020 16:35:02	...	10.10.5.182	859	0	▶	☰
9	33727	02/12/2020 12:34:39	02/12/2020 13:53:15	...	10.10.5.182	77	0	▶	☰
10	33722	02/12/2020 10:33:08	02/12/2020 11:14:11	...	10.10.5.182	4	0	▶	☰

Showing 1 to 10 of 39 entries (filtered from 50,328 total entries)

Previous

1

2

3

4

Next

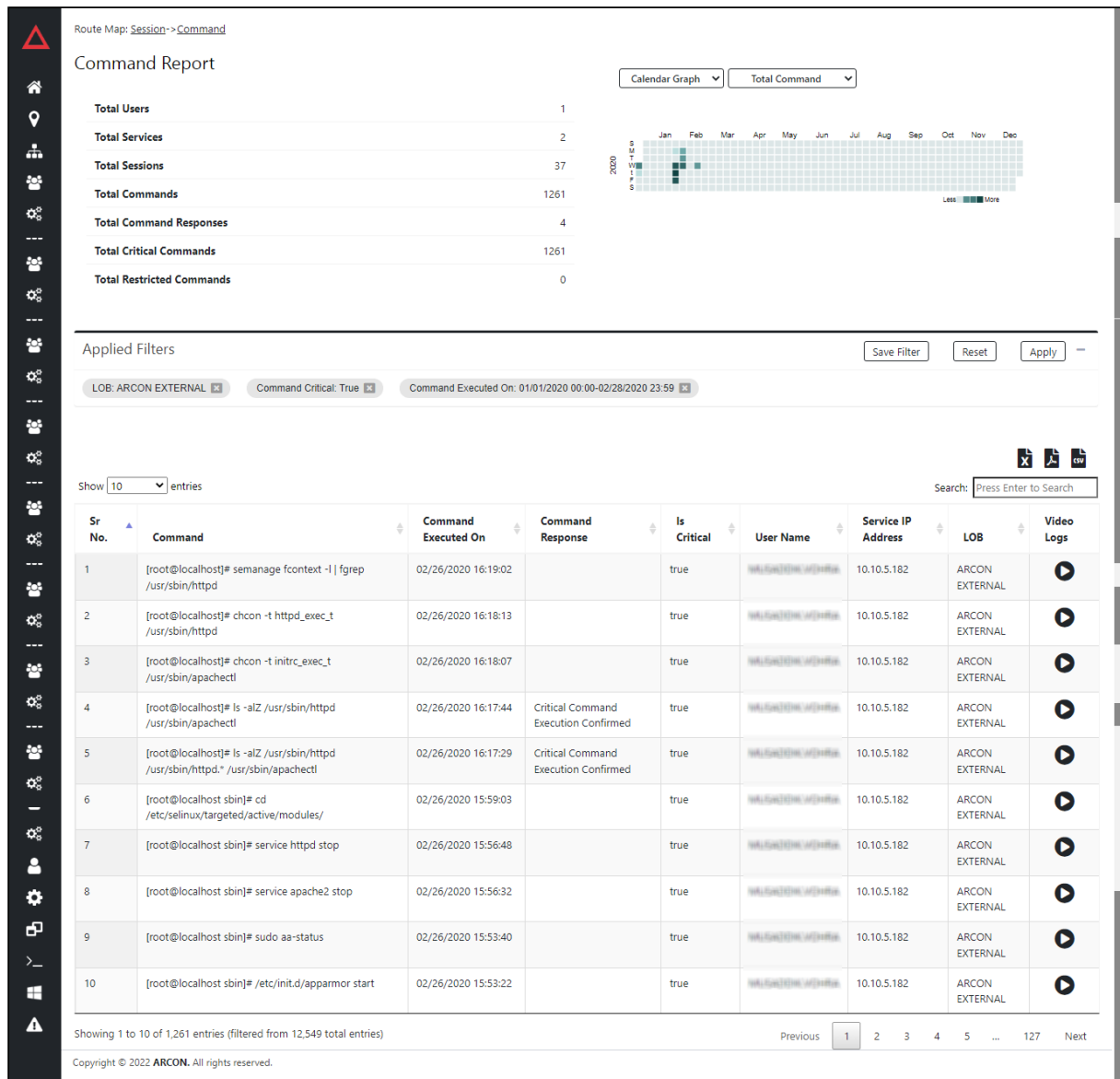
Copyright © 2022 ARCON. All rights reserved.

5.7 Command Report

Command Report gives us a list of commands fired on the server. It displays which command was fired, when was it executed, Command response, is it critical command, Username and IP address of the server from which it was fired. Before we walk through the Command Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Spection.

Features

- Video Logs- Video logs are captured for each command fired. At a time 4 video logs can be played.



Report builder Functionalities

- **Apply/Reset filter-** Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter-** The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries-** It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching-** The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting-** The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination-** The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.

- **Export to Excel, CSV, PDF-** All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo-** To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.7.1 Command Report Generation

Let us generate the Command report to see a list of all critical commands fired in the month of January and February where they belonged to ARCON External LOB.

We need to apply the following filters:- Critical Commands =True, Command Executed on = 01/01/2020-02/29/2020, LOB = ARCON External LOB.

Route Map: [Session](#) -> [Command](#)

Command Report

Calendar Graph

Total Command

Total Users	1
Total Services	2
Total Sessions	37
Total Commands	1261
Total Command Responses	4
Total Critical Commands	1261
Total Restricted Commands	0

Applied Filters

Save Filter

Reset

Apply

LOB: ARCON EXTERNAL

Command Critical: True

Command Executed On: 01/01/2020 00:00-02/28/2020 23:59

Show 10 entries

Search:

Sr No.	Command	Command Executed On	Command Response	Is Critical	User Name	Service IP Address	LOB	Video Logs
1	[root@localhost]# semanage fcontext -l fgrep /usr/sbin/httpd	02/26/2020 16:19:02		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
2	[root@localhost]# chcon -t httpd_exec_t /usr/sbin/httpd	02/26/2020 16:18:13		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
3	[root@localhost]# chcon -t initrc_exec_t /usr/sbin/apachectl	02/26/2020 16:18:07		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
4	[root@localhost]# ls -alZ /usr/sbin/httpd /usr/sbin/apachectl	02/26/2020 16:17:44	Critical Command Execution Confirmed	true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
5	[root@localhost]# ls -alZ /usr/sbin/httpd /usr/sbin/httpd.* /usr/sbin/apachectl	02/26/2020 16:17:29	Critical Command Execution Confirmed	true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
6	[root@localhost/sbin]# cd /etc/selinux/targeted/active/modules/	02/26/2020 15:59:03		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
7	[root@localhost/sbin]# service httpd stop	02/26/2020 15:56:48		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
8	[root@localhost/sbin]# service apache2 stop	02/26/2020 15:56:32		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
9	[root@localhost/sbin]# sudo aa-status	02/26/2020 15:53:40		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
10	[root@localhost/sbin]# /etc/init.d/apparmor start	02/26/2020 15:53:22		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	

Showing 1 to 10 of 1,261 entries (filtered from 12,549 total entries)

Previous

1

2

3

4

5

...

127

Next

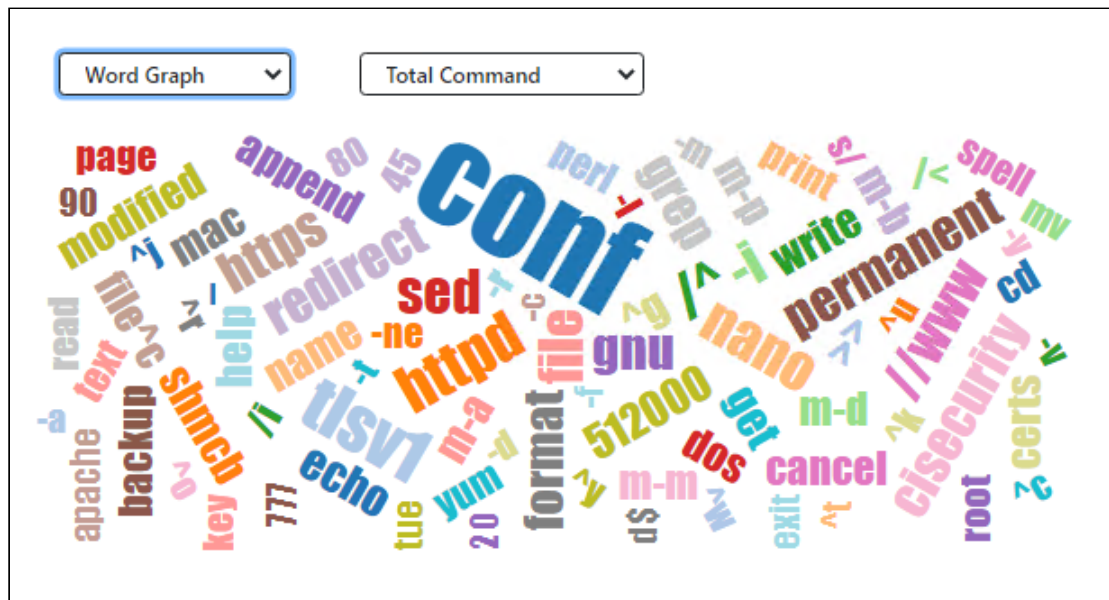
Copyright © 2022 ARCON. All rights reserved.

1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. Service Report statistic summary is displayed below.

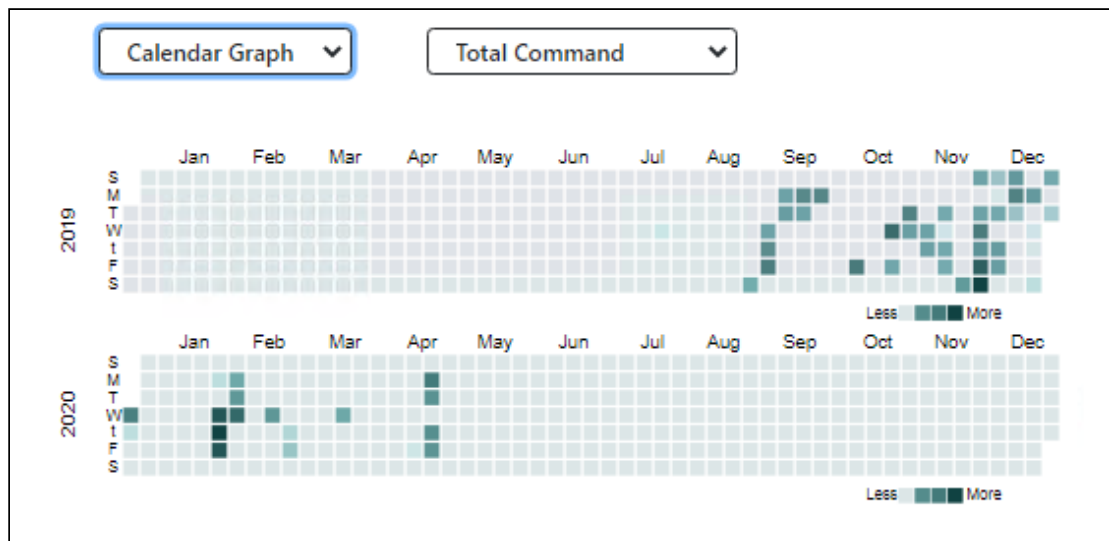
Command Report

Total Users	1
Total Services	2
Total Sessions	37
Total Commands	1261
Total Command Responses	4
Total Critical Commands	1261
Total Restricted Commands	0

2. **Graphs :-** Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are of two types
 - a. **Word Graph-** It displays the most frequently used commands in the word graph format where bigger font indicates more use of those commands. Filters can be applied on the command type i.e from Total command, Restricted command, Critical command.



- b. Calendar Graph-It displays the number of commands fired on a particular day. Filters can be applied on the command type i.e from Total command, Restricted command, Critical command. The dark box displays more command fired and light color indicates fewer commands fired on that day.



3. **Report table:-** The tabular report displays the record in a grid format. Video logs of commands can be viewed here.

Applied Filters Save Filter Reset Apply

LOB: ARCON EXTERNAL X Command Critical: True X Command Executed On: 01/01/2020 00:00-02/28/2020 23:59 X

Show entries Search:

Sr No.	Command	Command Executed On	Command Response	Is Critical	User Name	Service IP Address	LOB	Video Logs
1	[root@localhost]# semanage fcontext -l fgrep /usr/sbin/httpd	02/26/2020 16:19:02		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
2	[root@localhost]# chcon -t httpd_exec_t /usr/sbin/httpd	02/26/2020 16:18:13		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
3	[root@localhost]# chcon -t initrc_exec_t /usr/sbin/apachectl	02/26/2020 16:18:07		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
4	[root@localhost]# ls -alZ /usr/sbin/httpd /usr/sbin/apachectl	02/26/2020 16:17:44	Critical Command Execution Confirmed	true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
5	[root@localhost]# ls -alZ /usr/sbin/httpd /usr/sbin/httpd.* /usr/sbin/apachectl	02/26/2020 16:17:29	Critical Command Execution Confirmed	true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
6	[root@localhost/sbin]# cd /etc/selinux/targeted/active/modules/	02/26/2020 15:59:03		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
7	[root@localhost/sbin]# service httpd stop	02/26/2020 15:56:48		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
8	[root@localhost/sbin]# service apache2 stop	02/26/2020 15:56:32		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
9	[root@localhost/sbin]# sudo aa-status	02/26/2020 15:53:40		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	
10	[root@localhost/sbin]# /etc/init.d/apparmor start	02/26/2020 15:53:22		true	[REDACTED]	10.10.5.182	ARCON EXTERNAL	

Showing 1 to 10 of 1,261 entries (filtered from 12,549 total entries)

Previous 1 2 3 4 5 ... 127 Next

Copyright © 2022 ARCON. All rights reserved.

5.8 Process Report

Process Report gives us a list of processes in ARCON PAM. It displays the name, title timestamp, Username, type of User, Service IP Address, type of service, whether a process is restricted, and video logs. Before we walk through the Process Report let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Specion.

Features

- **Video Logs-** Video logs are captured for each processes. At a time 4 video logs can be played.

Session -> Command -> Process

Process Report

Calendar Graph

Total Users: 231
Total Services: 325
Total Sessions: 51226

Session - 51524 || TEJALSOLANKI

Session - 51524 || TEJALSOLANKI

Session - 51524 || TEJALSOLANKI

Session - 51524 || TEJALSOLANKI

6	Inactivated	12/05/2020 17:32:13	TEJALSOLANKI	Client	10.10.0.130	Windows RDP	False	▶
7	Activated	12/05/2020 17:30:19	TEJALSOLANKI	Client	10.10.0.130	Windows RDP	False	▶
8	Inactivated	12/05/2020 17:29:28	TEJALSOLANKI	Client	10.10.0.130	Windows RDP	False	▶
9	Activated	12/05/2020 17:28:24	TEJALSOLANKI	Client	10.10.0.130	Windows RDP	False	▶
10	Inactivated	12/05/2020 17:24:34	TEJALSOLANKI	Client	10.10.0.130	Windows RDP	False	▶

Showing 1 to 10 of 2,297 entries

Previous 1 2 3 4 5 ... 230 Next

Copyright © 2020 ARCON. All rights reserved.

Report builder Functionalities

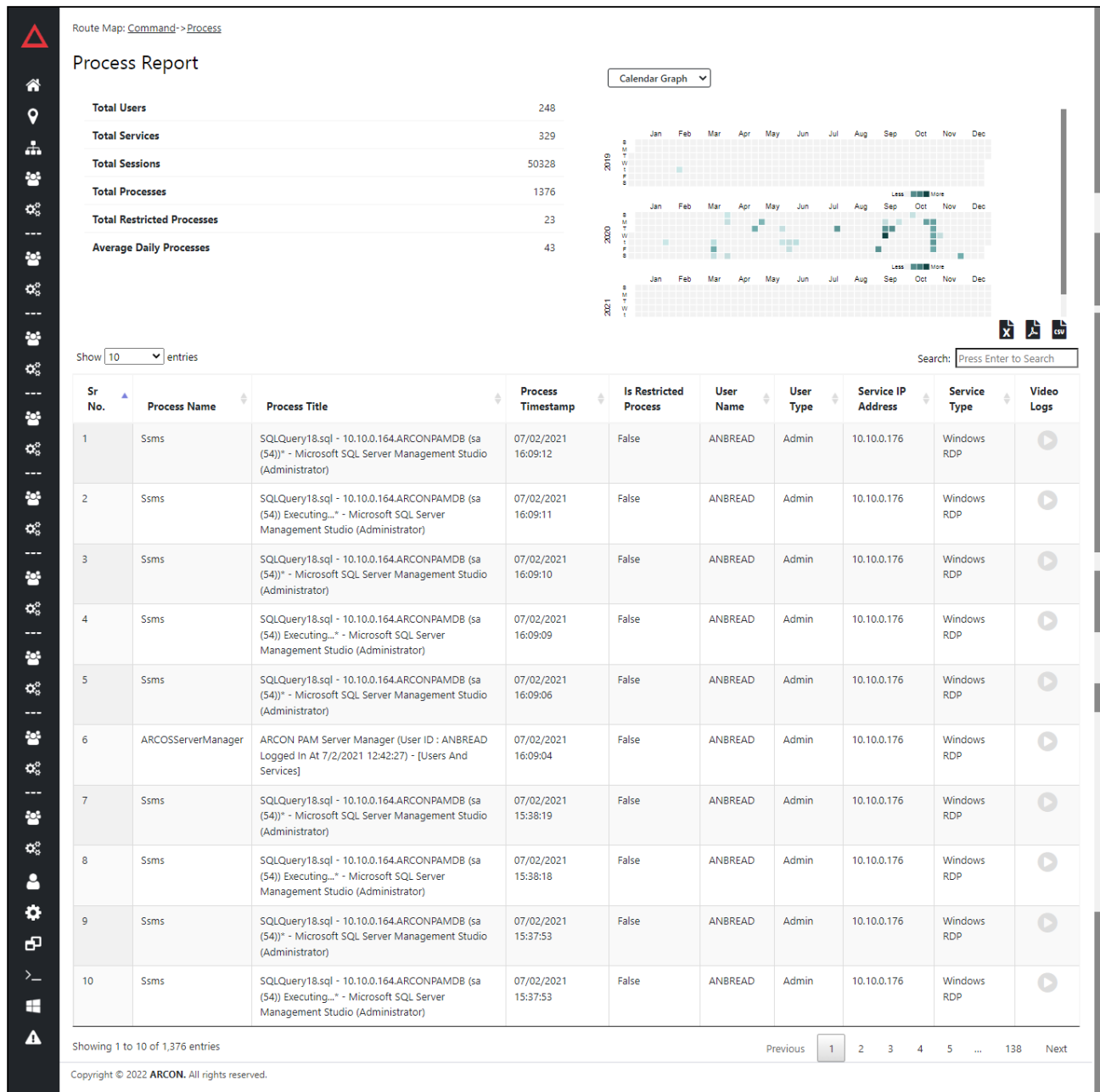
- **Apply/Reset filter-** Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter-** The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries-** It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching-** The search filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.

- **Sorting-** The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination-** The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF-** All the reports in ARCON Spection can be downloaded and exported in the XLSX, CSV and PDF format.
- **Watermark and Logo-** To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Spection API package.

5.8.1 Process Report Generation

Let us generate the Process report to see the list of all the processes.

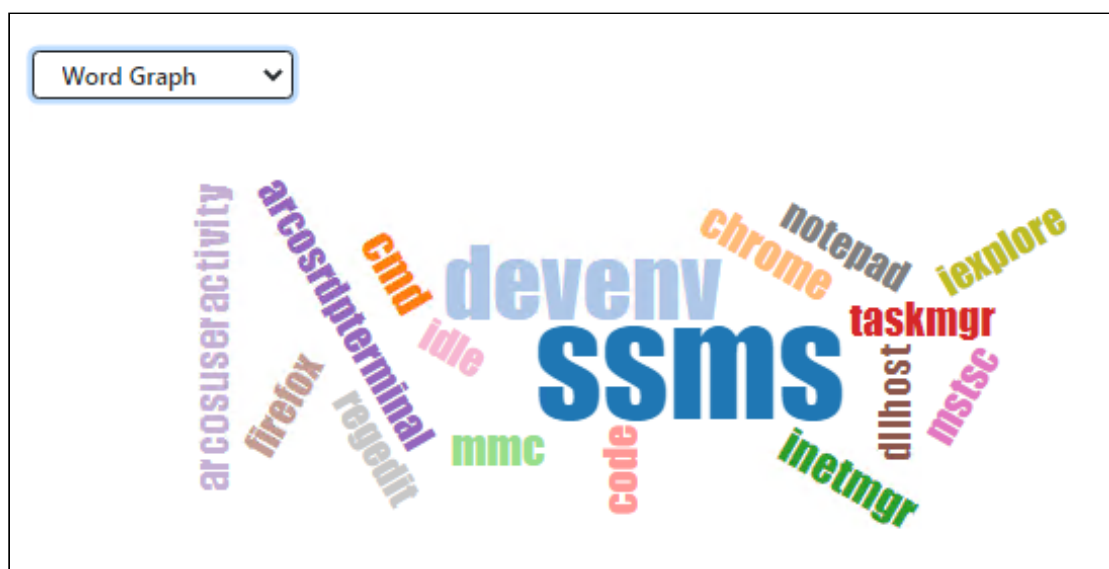
We do not apply any filters to generate the process report.



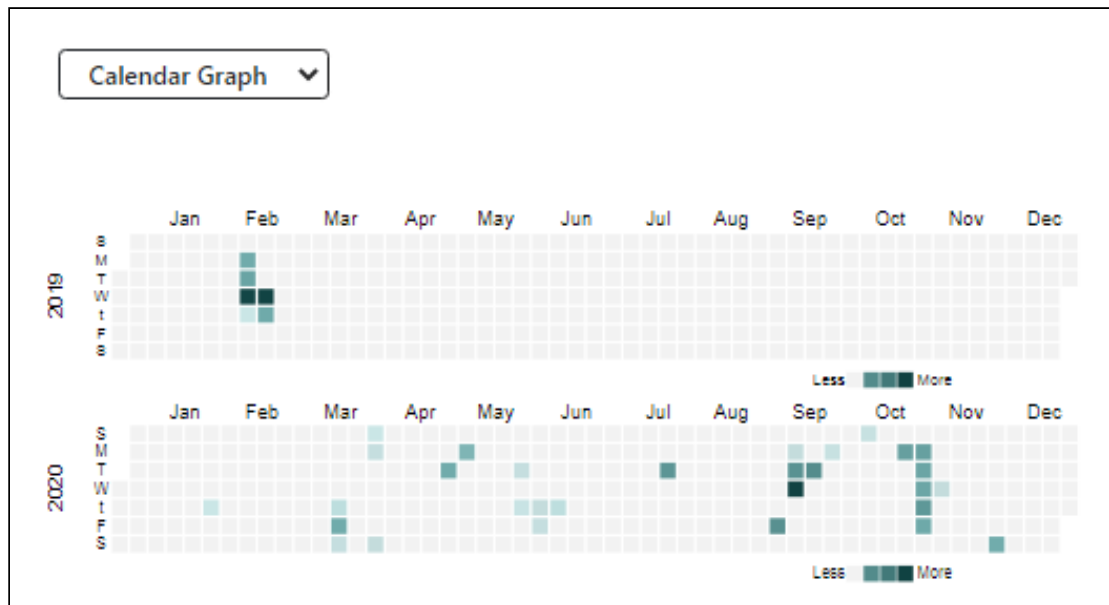
1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. Process Report statistic summary is displayed below.

Process Report	
Total Users	231
Total Services	325
Total Sessions	51221
Total Processes	2297
Total Restricted Processes	23
Average Daily Processes	63

2. **Graphs :-** Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The graphs are of two types
- Word Graph- It displays the most frequently used processes in the word graph format where bigger font indicates higher use of those processes.



- Calendar Graph-It displays the number of processes used on a particular day. The dark box displays more processes used and the light color indicates fewer processes used on that day.



3. **Report table:-** The tabular report displays the record in a grid format. Video logs of processes can be viewed here.

Show entries

Search:

Sr No.	Process Name	Process Title	Process Timestamp	Is Restricted Process	User Name	User Type	Service IP Address	Service Type	Video Logs
1	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 16:09:12	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
2	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 16:09:11	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
3	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 16:09:10	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
4	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 16:09:09	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
5	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 16:09:06	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
6	ARCOSServerManager	ARCON PAM Server Manager (User ID : ANBREAD Logged In At 7/2/2021 12:42:27) - [Users And Services]	07/02/2021 16:09:04	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
7	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 15:38:19	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
8	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 15:38:18	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
9	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 15:37:53	False	ANBREAD	Admin	10.10.0.176	Windows RDP	
10	Ssms	SQLQuery18.sql - 10.10.0.164.ARCONPAMDB (sa (54)) - Microsoft SQL Server Management Studio (Administrator)	07/02/2021 15:37:53	False	ANBREAD	Admin	10.10.0.176	Windows RDP	

Showing 1 to 10 of 1,376 entries

Previous 2 3 4 5 ... 138 Next

Copyright © 2022 ARCON. All rights reserved.

5.9 Outside Access Report

Outside Access Report is a report which displays details of outsiders (unauthorized users) trying to access the services. Outside Access reports help to generate a graphical view and the exact count of clients accessed outside PAM based on the year/month defined. Before we walk through the Outside Access report, let us understand some common reporting functionalities which are applicable to the reports in ARCON PAM Specion.

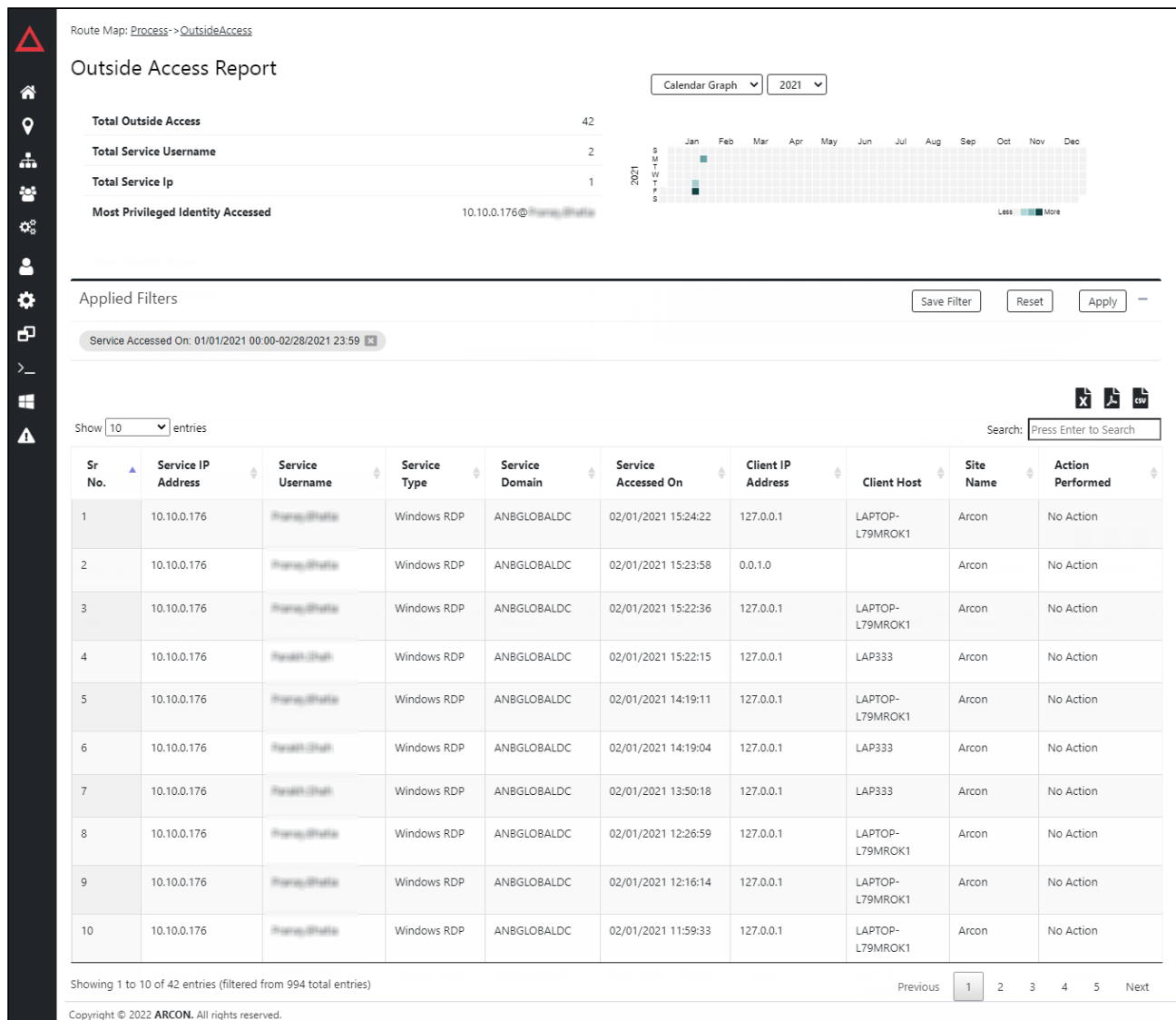
Report builder Functionalities

- **Apply/Reset filter**- Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top and click **Apply**. To **Reset** all the changes to default click **Reset**.
- **Save/Pin filter**- The filters can be saved and pinned to access the report directly and eliminate redundant selection all the time.
- **Show Entries**-It displays the number of rows selected from the dropdown in the reporting grid.
- **Searching**-The searching filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you are interested in seeing.
- **Sorting**- The column names of the reporting table have the sorting functionality which arranges the data alphabetically or numerically in ascending/descending order.
- **Pagination**-The Report grid at the bottom is paginated it prints all the data in a table, no matter how long. One can further scroll through all the rows through the stroll bar on the right.
- **Export to Excel, CSV, PDF**- All the reports in ARCON Specion can be downloaded and exported in the XLSX, CSV, and PDF format.
- **Watermark and Logo**- To protect the content and ownership of the PDF reports organizations can set their watermark and company logo in the Specion API package.

5.9.1 Outside Access Report Generation

Let us generate the Outside Access report to see a list of all client details accessed outside PAM in the month of January and February.

We need to apply the following filter:- Service Accessed on = 01/01/2021- 02/28/2021.

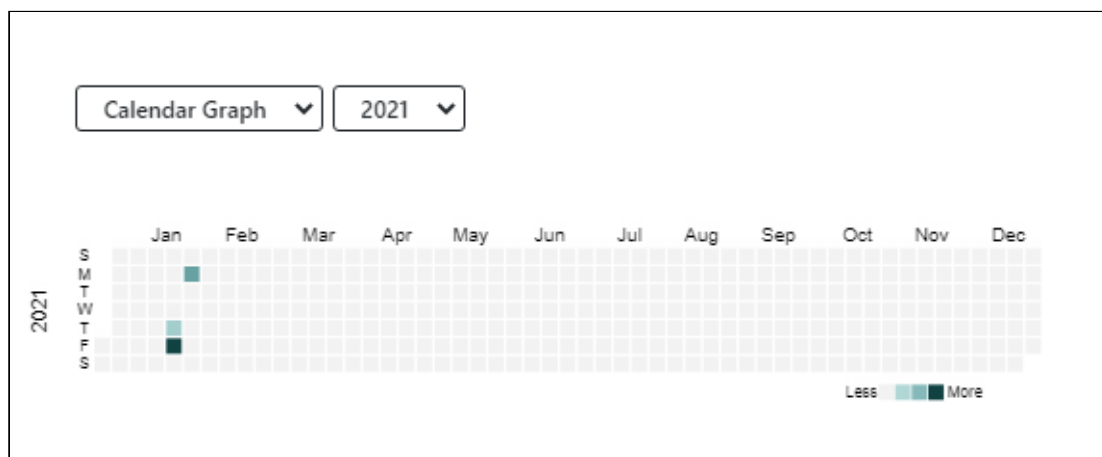


The Outside Access report consists of 3 major sections which are described below.





1. **Statistics** :- Statistics give us an accurate count of the number of different attributes present. Outside Access Report statistics summary is displayed below.

Outside Access Report	
Total Outside Access	42
Total Service Username	2
Total Service Ip	1
Most Privileged Identity Accessed	10.10.0.176@Pammy@Shakti

2. **Graphs :-** Graphical representations help in visualizing large volumes of data in an understandable and coherent way. The Calendar graph displays the total number of outside accesses of the respective day/month. Filters can be applied based on the year. The dark box displays higher outside accesses and light color indicates less outside accesses on that day.



3. Report table:- The tabular report displays the records in a grid format.

Applied Filters									
Service Accessed On: 01/01/2021 00:00-02/28/2021 23:59 									
<div> <div>    </div> <div> Show <input type="text" value="10"/> entries </div> <div> Search: <input type="text" value="Press Enter to Search"/> </div> </div>									
Sr No.	Service IP Address	Service Username	Service Type	Service Domain	Service Accessed On	Client IP Address	Client Host	Site Name	Action Performed
1	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 15:24:22	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
2	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 15:23:58	0.0.1.0		Arcon	No Action
3	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 15:22:36	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
4	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 15:22:15	127.0.0.1	LAP333	Arcon	No Action
5	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 14:19:11	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
6	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 14:19:04	127.0.0.1	LAP333	Arcon	No Action
7	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 13:50:18	127.0.0.1	LAP333	Arcon	No Action
8	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 12:26:59	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
9	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 12:16:14	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
10	10.10.0.176	Pranshu@Hestia	Windows RDP	ANBGLOBALDC	02/01/2021 11:59:33	127.0.0.1	LAPTOP-L79MROK1	Arcon	No Action
<div> Showing 1 to 10 of 42 entries (filtered from 994 total entries) </div> <div> Previous 1 2 3 4 5 Next </div>									
Copyright © 2022 ARCON. All rights reserved.									

Privileged Access Management Suite



No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means such as electronic, mechanical, photocopying, recording, or otherwise without permission.