TAILORING INSIGHTS: CREATING PERSONALIZED DASHBOARDS FOR USERS IN A MULTI-TENANT ENVIRONMENT



In a managed service provider (MSP)-centric environment, managing the diverse needs of multiple end users within a single tenant environment can be challenging. However, the benefits of personalized dashboards for these end users are significant. Each end user brings unique requirements and preferences for visualizing their information technology (IT) infrastructure within this domain. This is where the multi-tenancy dashboard becomes invaluable. Using tools like **BMC Helix Access Controls**, MSPs can now seamlessly create personalized dashboard views for individual end users, revolutionizing how data is accessed, analyzed, and utilized within a unified framework.

We've had inquiries regarding the feasibility and logistics of implementing personalized dashboards within a multi-tenant environment; one resounding question echoes: "Can it truly be done?" How do you navigate the process of setting up and managing dashboards tailored to multiple end users' individual roles and preferences?

This blog is designed to address your concerns. We will guide you through the practical application of creating and managing dashboards with distinct users. The answer to the question is a resounding "Yes, it can be done!" We will equip you with the necessary steps and insights to make this process a reality in your multi-tenant environment.

Creating a User Group

Let's start by creating a User group. For this blog, we will create a User group for the end customer, "XYZ Manufacturing." In the next steps, you'll discover how easy it is to create personalized

dashboards based on your end user, empowering you to tailor the experience to their unique needs.

Here is a screenshot showing the group creation. As the BMC Helix tenant administrator, you will first go into the portal:

bmc helix	Portal	Home	User access 🗸	Configure 🗸	Report				
			🔒 Roles and pe	ermissions					
			坐 User groups						
Helix	Portal		👃 Users and ke	eys					
All your	All your Helix applications at your fingertips.								
Featured	Featured applications								
				··					
			Figure 1. Ma	am screen.					

As the administrator for the XYZ Manufacturing company, you will then click on Add group and create the specific User group. The image below shows the administrator creating TestGroup1.

bmchelix Portal	Home	User access 🗸	Configure ~	Report		:	· ?.	Ť^	L.
User groups									
Add group									
1 row shown						Q	Test		×
Group Name 🍦				Type 🌲	Actions				
TestGroup1				Local	Actions 👻				

Figure 2. User groups.

Now that the administrator has created a new User group, they will need to add the permissions. The administrator simply clicks on Actions -> Assigned, and assigns the User to the Group:

1 row showr TestGroup1 User n	n name User login	Q Search
Sayan	Banerjee sbanerje	
Assignments		
Users Select 1 assigned		



Next, the administrator will want to check the User's role. This is easily done by going to the BMC Helix portal landing page, clicking the User access tab, going to the Users and keys page, and searching for the User.

Source Home User access	✓ Configure ✓ Report						?-	4 ?	L.
Users and keys									
Manage user accounts and tenant access keys.									
Users Access keys									
Add user									
1 row shown 🝸 Filters 👻							Q sba	nerje	×
User name 🔅	Login ID 🗘	Activation date 🔅	Source	Status 🗘	Actions				
Sayan Banerjee	sbanerje	Aug 11, 2023 at 01:47 PM	External user	ENABLE	Actions •				

Figure 4: Users and keys.

Now that the administrator sees the User, they can simply click on Actions -> User options to see which User groups and Roles are assigned to them. By selecting either the Groups or Roles assignment area, the administrator can quickly validate that they are assigned correctly.

User options	×	User groups	×
External user Sayan Banerjee		2 rows shown Group Name Licensed User	Q Search
Assignments		TestGroup1	
Groups 2 assigned	Select		
Roles 1 assigned	Select		6
			?

Figure 5: User options.

Creating an Authorization Profile

One of the next things you will want to do as the administrator is to create an authorization profile for this User group (TestGroup1). By creating this authorization profile, you ensure that the Users in this Group only have access to the appropriate XYZ Manufacturing company information.

Here's how you do this: Launch the BMC Helix Operations Management console from the BMC Helix portal landing page. Then, navigate to the Administration Authorization profile, and you will see the Authorization Profile Test_AutoProf1, which we have created for User group TestGroup1. In your case, this needs to be created using the "Create" button option.

Monitoring ~ Configuration ~	Administration ~		III. 🛄
		Name 👻 Test	× Q ?
			Create
	Monitoring ~ Configuration ~	Monitoring Configuration Administration	Monitoring Configuration Administration Name Test

Figure 6. Authorization profiles.

The next step is to add and associate the User group we created.

bmc helix	Operations Management	Monitoring ~ Configuration ~ Administration ~	l
← Profile	Details		•
Authorization Pr Test_AuthProf1	rofile Name	Total User Groups 1	
User Group	ps Objects		
Associated User	Groups (required) <table-cell-rows> Add</table-cell-rows>		
✓ TestGroup1			

Figure 7. Profile details.

In this case, we have selected Microsoft Windows Servers as the PATROL Solutions and then assigned a specific Device and Group. The Device name and Group name will vary depending on customer requirements.

bmchelix Operations Management	Monitoring Configuration Administration	II. 🛄
← Profile Details		0
Authorization Profile Name Test_AuthProf1	Total User Groups 1	
User Groups Objects		
Associated Objects		
Types (4)	Objects (1) PATROL Solutions	
PATROL Solutions	Microsoft Windows Servers	
PATROL Agent ACLs		
Devices		
Groups		



≽bmchelix (Operations Management	Monitoring ~ Configuration ~	Administration ~	Ť	L,
← Profile [Details				0
Authorization Pro Test_AuthProf1	file Name	Total User Groups 1			
User Groups	Objects				
Associated Object	s				
Types (4)			Objects (1) : Devices		
PATROL Solu	tions		vl-pun-dombl107		
PATROL Ager	nt ACLs				
Devices					
Groups					

Here we are showing the selection of the Group Windows Servers.

bmchelix Operations Management	Monitoring Y Configuration Y A	dministration ~		L.
← Profile Details				8
Authorization Profile Name Test_AuthProf1	Total User Groups 1			
User Groups Objects				
Associated Objects				
Types (4)		Objects (1) : Groups		
PATROL Solutions		Windows Servers		
PATROL Agent ACLs				
Devices				
Groups				8

Figure 9a.Windows Servers.

Setup Complete

As you've seen so far, this has all been straightforward to implement. Let's now log into the BMC Helix portal as the user and see how it shows up. Here's the dashboard, with all the devices that the user has available to them displayed.

bmchelix Op	perations Mana	gement	Monitoring 🗸	Configuratio	on ~
Devices :					
All Devices 2	Server 2				
Count of Devices wit	th Events				
Open 2	Acknowledged Assig		ned	Blackout Closed 2	
Critical 2	Major 1	Mino 1	or	Warning	Information 2
Tile View 🚦 Sort by Se	verity				
Server vl-pun-dombl107	Server clm-pun-u5s	5260			
	1				
	1		5		

Figure 10. Main dashboard.

Based on the rules the administrator has put in place, this user can only see the two devices that were assigned.

The user can see deeper insights from the dashboard by clicking on one of the servers (for this example, we've clicked into the vl-pun-dombl107 server).

bmc	helix Opera	ations Ma	anagemen	t Monitoring	g 🎽 Cor	nfiguration ~							 ~	S.
← D	evice Detai	ils												▶ 0
Device	Name					Event Summary								
vi-pu	in-dombi107	•					6	•	•	A	0			
Type Server		Monitors 49		Agents 1		Open		1		16	1			
DNS N	lame		IP Address			Acknowledged								
vl-pun-	-dombl107		172.20.29.5			Assigned								
						Blackout								
E	Events Mo	onitors	Agents											
Table Vie	w Hierarchy													Q
Monitor	Name				Monito	or Type			E	vents Co	unt	Blackout		8
Linux	OS				Linux C)S				0				
> vl-pur	n-dombl107:3981				PatrolA	gentHealthMonitor				0				

Figure 11. Deeper insights.

Once on the Device Details page, the user can click on the three dots beside the Device Name and then click on the "Launch Dashboard" pop-up to delve into all of the performance details:

bmchelix Operations Management	Monitoring V Configuration V	
← Device Details		
Device Name vl-pun-dombl107 :		Event Summary
Launch Dashboard Type Server 49	Agents 1	Open
DNS Name vl-pun-dombl107	IP Address 172.20.29.5	Acknowledged Assigned
		Blackout
Table View : Hierarchy :		
Monitor Name	Monitor 1	Гуре
> Linux OS		
> vl-pun-dombl107:3981 PatrolAgentHealthMoni		

Detailed Dashboard View

Once the user has clicked on Launch Dashboard, the system will default to the same device and show the CPU utilization, Memory usage, Disk usage, Network bandwidth utilization, and related events for this device.



Figure 13. Performance details.

Conclusion

As you can see, creating and managing multiple end users with personalized dashboards is quite simple. Using BMC Helix User group and Authorization profiles, the administrator can easily create the views needed to support personalized dashboards based on the user profiles. We hope this process walk-through will provide you with the guidance you have been asking for as you create your dashboards in your environment.

We are also here to answer any questions you might have; please feel free to reach out to us:

- <u>sayan_banerjee@bmc.com</u>
- anmol_rastogi@bmc.com