Hewlett Packard
Enterprise

HPE Application Performance Management

Software Version: 9.30

Multi-Tenancy Using APM - Best Practices

Document Release Date: December 2016
Software Release Date: July 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2005 - 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

HPE Software Integrations and Solutions

Visit the Integrations and Solutions Catalog at **https://softwaresupport.hpe.com/km/KM01702731** to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Contents

Introduction 5
Chapter 1: Scope and Motivation 6
Chapter 2: What is a Tenant? 7
Chapter 3: What is Multi-Tenancy? 8
Chapter 4: Solution Overview 9
Chapter 5: Use Cases 11
Step-by-Step Configurations 12
Chapter 6: Configuration Changes in the Tenant's CMS 13
Chapter 7: Configuration for End User Monitoring 18
Chapter 8: Create Views in APM 19
Chapter 9: Create MyBSM Pages 23
Chapter 10: Configure Users and Permissions 24
Chapter 11: Multi-Tenancy and Other Data Collectors 26
Send Documentation Feedback 27

Introduction

Chapter 1: Scope and Motivation

Multi-tenancy means different things to different people. Different service providers have different multi-tenancy needs (for example SaaS – Software as a Service, MSP – Managed Services Provider, or IaaS – Infrastructure as a Service), and there may be shared or split ownerships between service providers and clients.

The implementation of global system integrators like MSP, and the common use of the APM platform in a shared services environment, make it necessary to provide multi-tenant capabilities in a shared services platform. The following use cases were identified to demonstrate the multi-tenant capabilities of APM in a shared service platform.

This document provides the following:

- Definition of multi-tenancy, solution overview, and high level architecture of multi-tenancy.
- Use cases supporting multi-tenancy in APM.
- Detailed explanations on how to configure APM to provide multi-tenancy capabilities.

Chapter 2: What is a Tenant?

A **tenant** is a set of people (customers, service providers, or suppliers), whose access to data in support of customer contracts is managed as a collective whole. It is commonly referred to as an organization.

In the world of enterprise systems, a tenant is referred to as a customer receiving organization (CRO). Tenants are managed as part of the customer on-boarding process of the service provider.

For larger customers, a tenant can be defined based on business unit, contract segment, or geography, depending on contract entitlement. For example:

- Acme Manufacturing vs. Acme Sales
- Acme Web Hosting vs. Acme Workplace Services
- Acme North America vs. Acme Europe

Note that a user can be associated with more than one tenant; this is common for service provider personnel, but less common for customer personnel. A tenant is not a user group or resource group.

Chapter 3: What is Multi-Tenancy?

Multi-tenancy refers to a principle in software architecture whereby a single instance of software runs on a logical system and serves multiple client organizations (tenants), thereby increasing resource utilization and reducing operational complexity and cost.

Multi-tenancy is contrasted with a multi-instance architecture, whereby separate software instances (or hardware systems) are set up for different client organizations. Multi-instance architecture increases the costs to clients and support organizations. Supporting multi-tenancy within a single system reduces these costs by leveraging common infrastructure and support models.

The advantages of multi-tenancy are not universally supported within the software industry, and this may be a source of competitive differentiation.

Chapter 4: Solution Overview

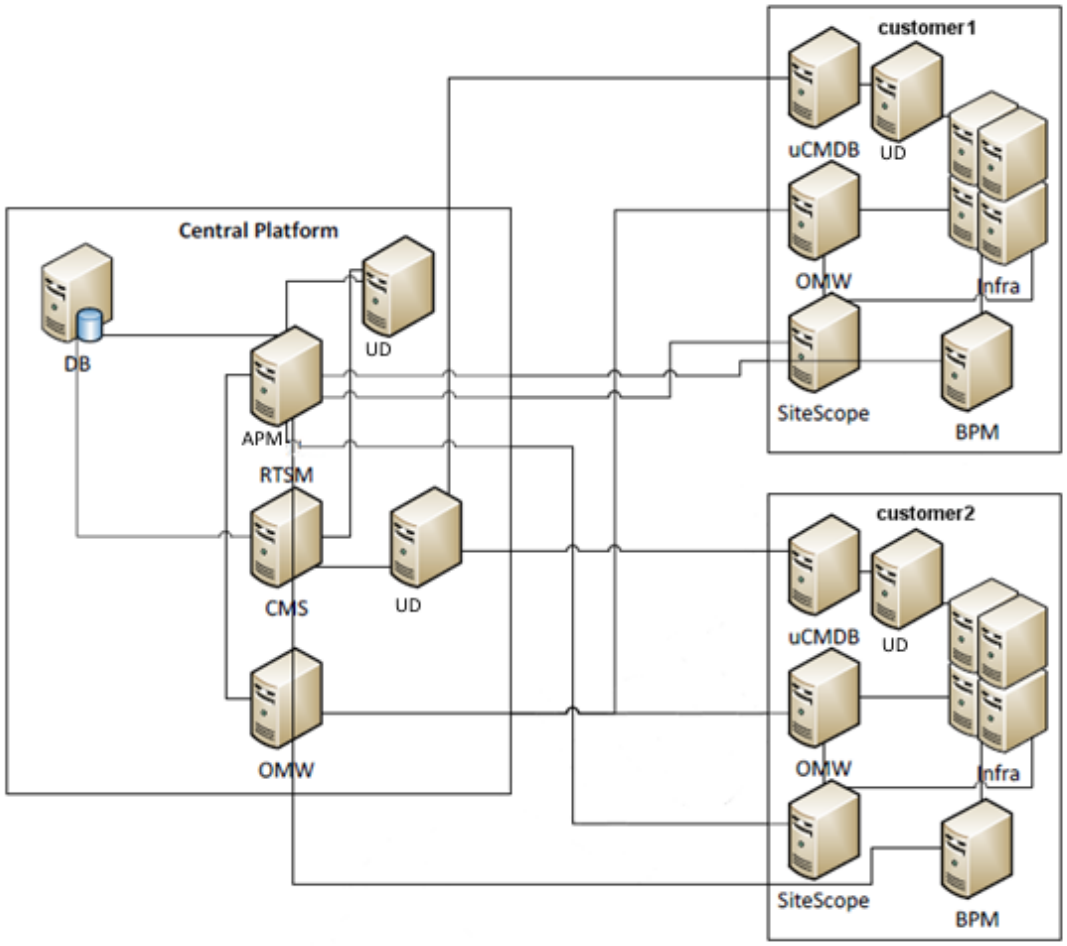
APM does not support multi-tenancy out-of-the-box. This document describes the configuration steps required to enable APM to support multi-tenancy use-cases.

The solution is based on the following:

- **Tenant Management.** Each tenant's data is identified within APM by a dedicated attribute; this is the foundation of the entire solution. In some cases this attribute is automatically enriched, but in some cases the MSP administrator must update this attribute manually. This attribute identifies the tenant who owns the element, which means that the element is managed under the lifecycle of that tenant.
- **Data-to-Tenant Relationship.** All the elements in APM - CIs, events, views, and so on - are related to one (and only one) tenant. Based on this information, data can be filtered in the different APM applications to show data for each tenant; for example you can filter events or RTSM views based on the tenant attribute.
- **Security Management.** Using the APM security model you can set permissions for different resources; APM allows you to assign different permissions to different user groups. This can be used to define different permissions for different tenants. This security model is managed by the MSP administrator, and will probably be the most significant area requiring administration in the multi-tenancy solution on top of APM.

The solution architecture is designed to address the use cases described in the following section. The main concept of the solution architecture is based on a local IT Operations environment for each customer, which is monitored by different monitoring tools (such as SiteScope, BPM), and discovered by UD. All this information is then sent to a central APM/CMS platform, and accessed by different tenants.

The diagram below is one example of a deployment scenario; there are many variations to multi-tenancy but the basic concept will be similar. For example, some of the monitoring products such as BPM or SiteScope can also be leveraged across tenants (using remote monitoring); in this case they are configured and managed by the service provider using the central APM platform, and the monitored data is accessed through the various APM applications (Event Console, Service Health and so on).


customer1
uCMDB
UD
OMW
Infra
SiteScope
BPM
Central Platform
DB
UD
APM
RTSM
CMS
UD
OMW
customer2
uCMDB
UD
OMW
Infra
SiteScope
BPM

Chapter 5: Use Cases

The multi-tenancy solution should provide the following capabilities:

Dashboard

- **Different Dashboards for Different Tenants.** Show all IT components managed by the various monitoring tools (SiteScope, BPM, and so on) in separate views for each tenant. This includes Service Health, Event Management, Reports, SLM, and so forth.
- **Integrated Dashboard for the Operations Team.** Show integrated views with data from all tenants, to be used by the MSP Operations team.
- **Event Correlation.** Provide event correlation for each tenant independently.

uCMDB

- **Discovery and Integration.** Provide integration of multiple CMDBs with one CMS system.
- **Independent Discovery.** Provide discovery and mapping capabilities for each tenant independently.

Monitoring

- **Distributed Monitoring.** Integrate all remote monitoring platforms using a central APM platform.
- **Event Views.** Provide different event views for different tenants.
- **Reports.** Provide scheduled reports for different tenants.

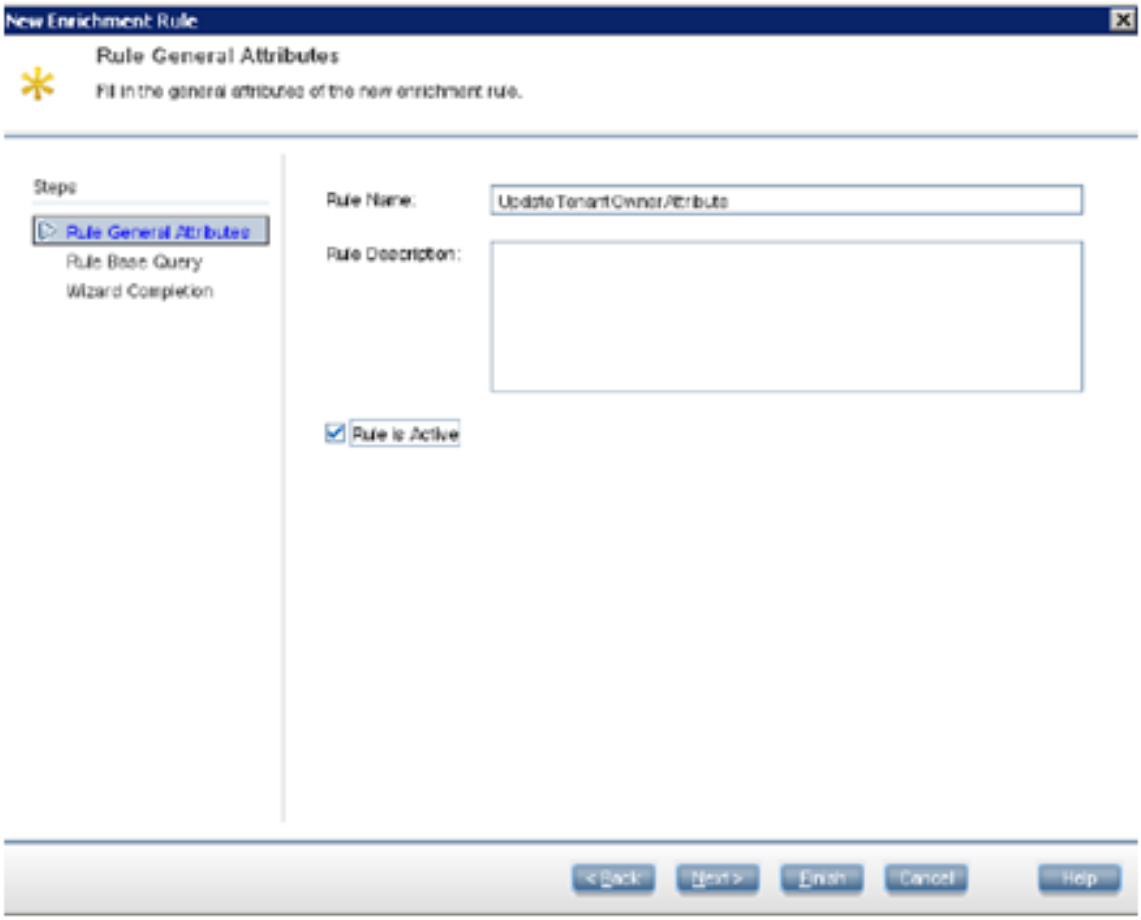
Step-by-Step Configurations

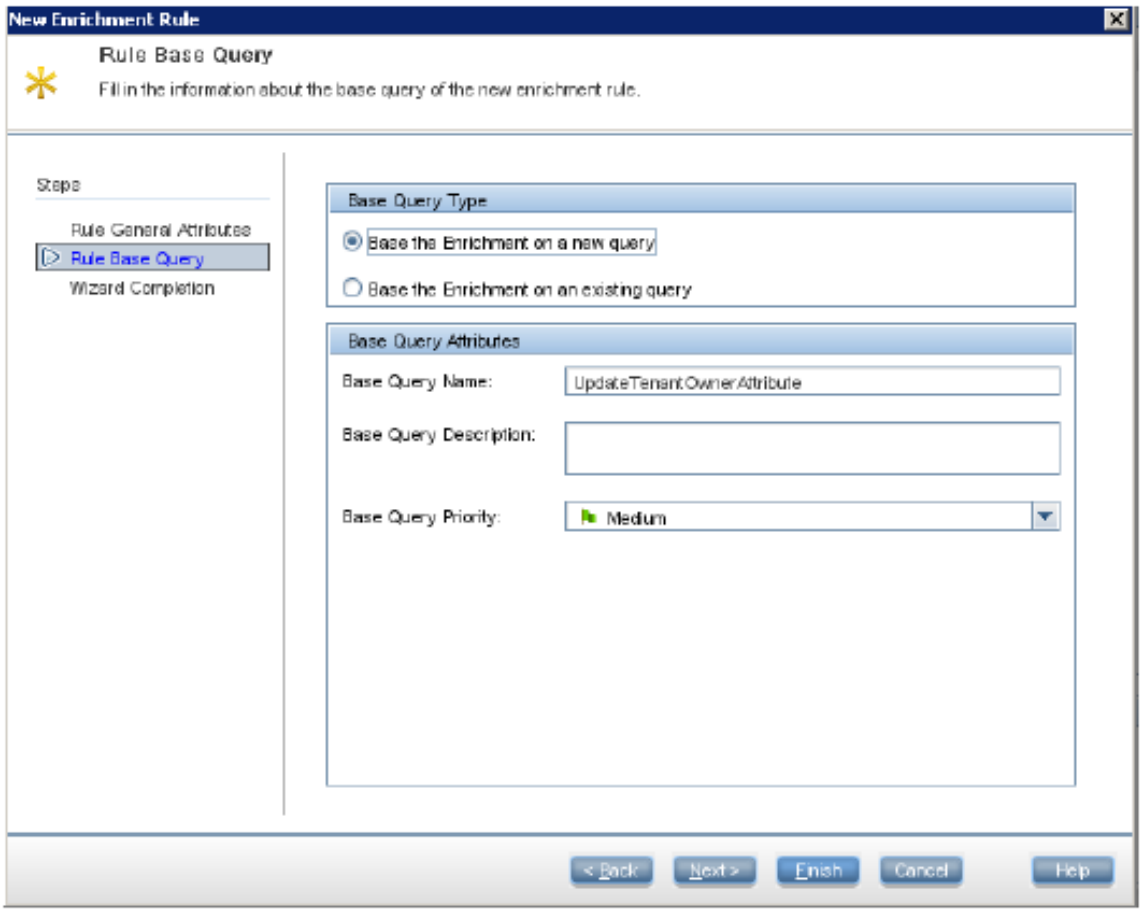
Chapter 6: Configuration Changes in the Tenant's CMS

If your tenant will have discovery capabilities, the DDM probe in the tenant environment should be connected to the tenant's (local) CMS. You can then synchronize the relevant topology from this CMS into the central APM/CMS.

To do this, you must perform the following configuration changes on each tenant's CMS:

1. Create an enrichment rule which will fill the Tenant Owner attribute for each CI in this local CMS. This is necessary so that when you synchronize CIs from the local CMS to the central CMS, the CIs will be associated with the correct tenant.
   a. In each tenant's CMS, access **Modeling > Enrichment Manager**.
   b. Create a new enrichment rule with a meaningful name. Activate the rule, and select **Base the Enrichment on a new Query**, as seen in the following images:

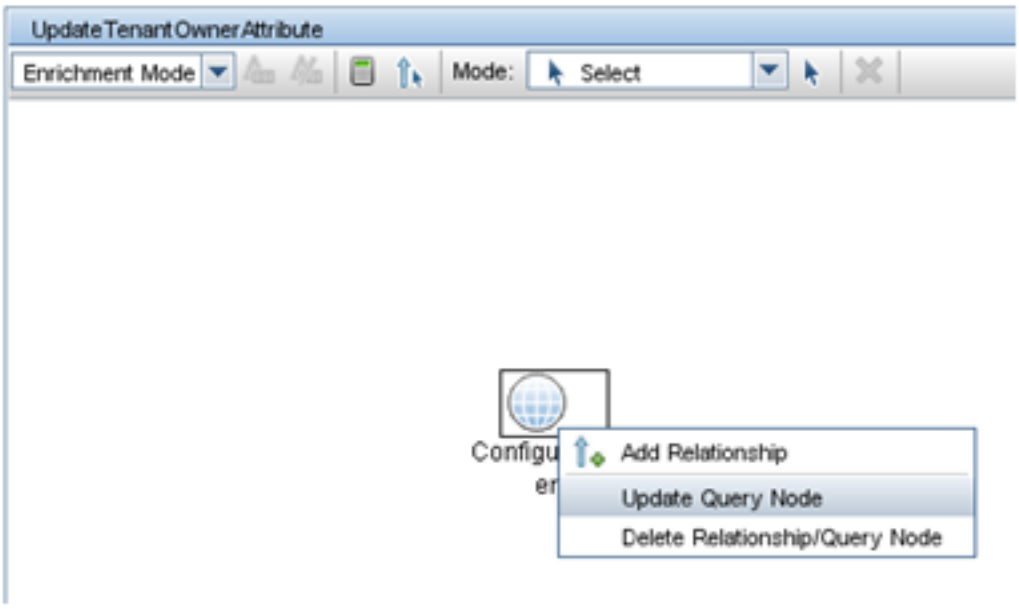




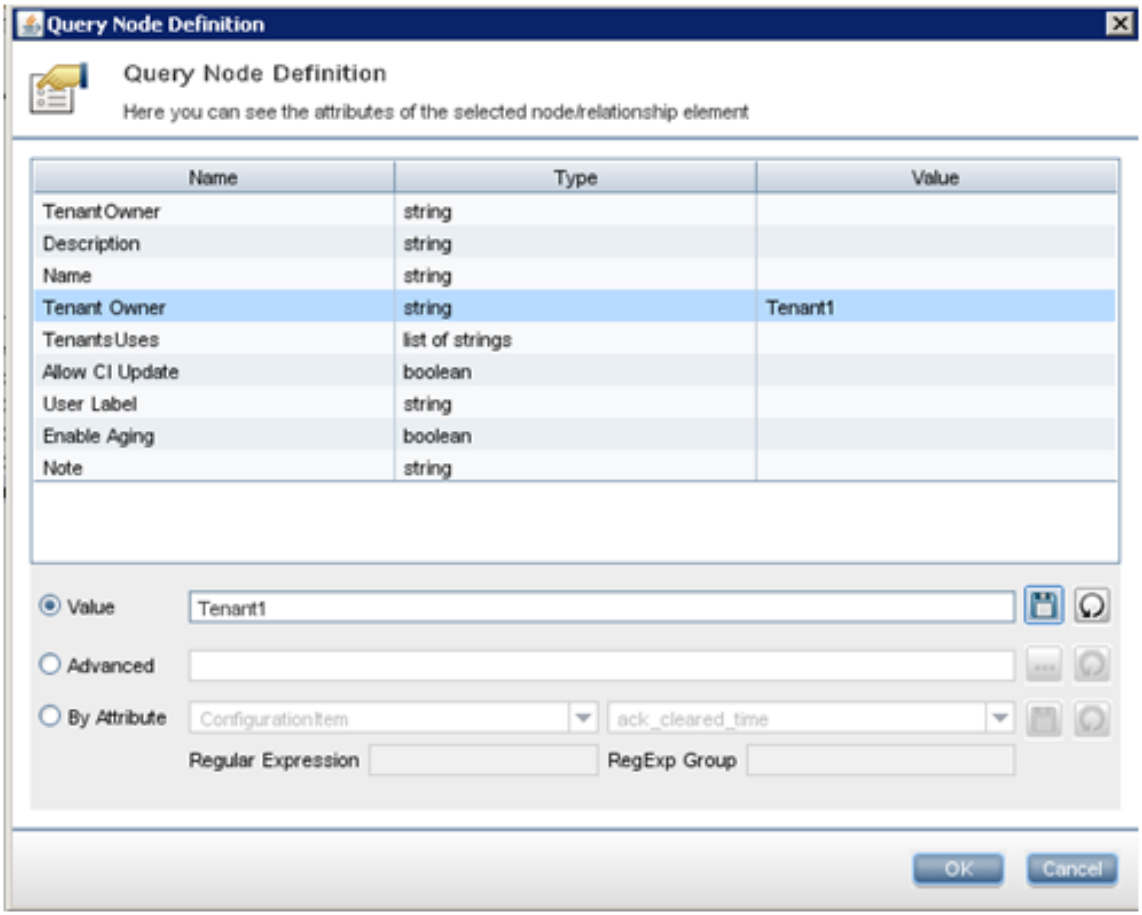
c. Click **Finish**.

d. In **Query Mode**, select the **Configuration Item** CI type.

e. Within **Enrichment Mode**, right-click **Configuration Item** and select **Update Query Node**:



f. Select the attribute you want to update; enter its value, and click **Apply**:



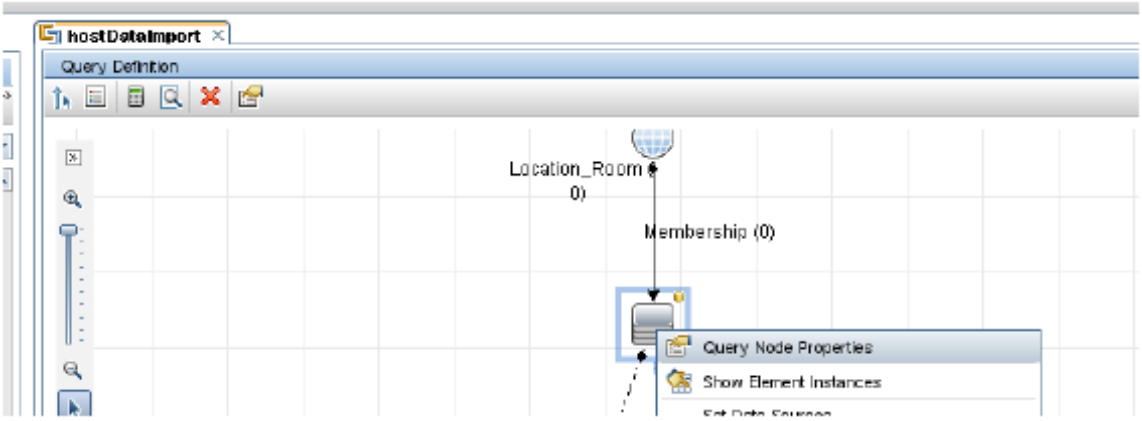
g. Click **OK** to save the enrichment rule and activate it.

h. You can validate the enrichment results in IT Universe Manager.

2. Modify the Integration TQLs that you will use to synchronize topology from the local CMS to the central CMS, to also synchronize the Tenant Owner attribute:

a. On each tenant's CMS, within **Modeling Studio > Resource Type** access **Queries**.

b. In each Integration TQL, right-click each of the query nodes and select **Query Node Properties**:



c. In the **Query Node Properties** dialog box, open the **Element Layout** tab.

d. Add the **Tenant Owner** attribute to the query.

e. Click OK to save your changes.

f. Repeat the above step b - step e for each element in the query, and then click **Save** in the left pane.

3. Within the central APM, define an integration point to the tenant's CMS in order to synchronize CIs into APM:

a. Within the central APM, access **Admin > RTSM Administration > Data Flow Management > Integration Studio**.

> **Note:** You must connect the Data Flow Probe to APM before performing these steps, and configure credentials to CMS in Probe administration. This is done using the Data Flow Probe set up; for details refer to the Data Flow Management Guide.

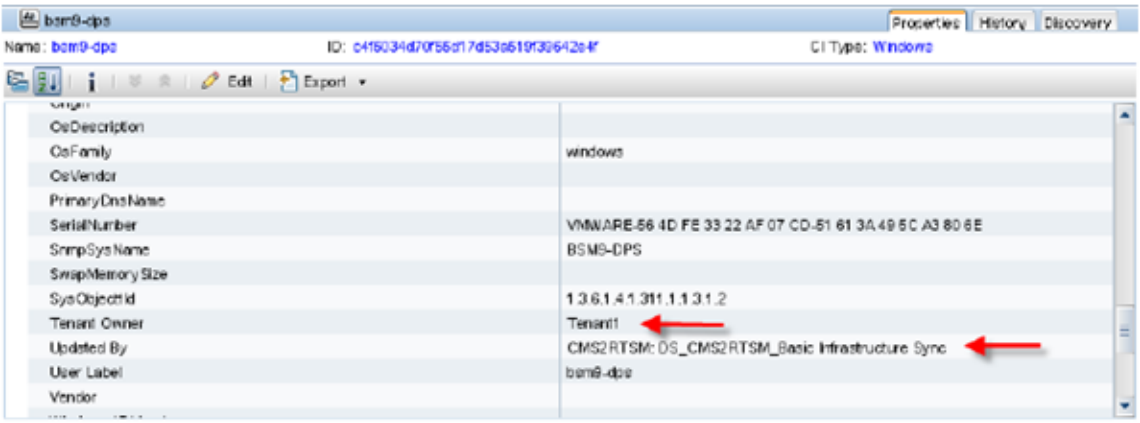
b. Create a new integration point:

c. Add new jobs; for each job select the Integration TQL for which you configured Layout Settings in

step 4 above.

d. Save the integration point, and perform full synchronization.

e. Within IT Universe Manager, check that you received CIs from the local CMS, and that they contain the Tenant Owner attribute:



Note: In your deployment scenario, if each tenant's DDM will be connected directly to the central APM, you need to employ a different approach to enrich the Tenant Owner attribute in APM, such as using an Enrichment Rule.

Chapter 7: Configuration for End User Monitoring

You can configure EUM-level permissions for users to restrict access to tenant-specific applications (see "Create MyBSM Pages" on page 23). However, to separate the applications and application views in RTSM, you must add the **TenantOwner** attribute manually for all the Business Applications. This needs to be done once for each Business Application CI; it can be done before or after creating the Business Application configuration in EUM Administration.

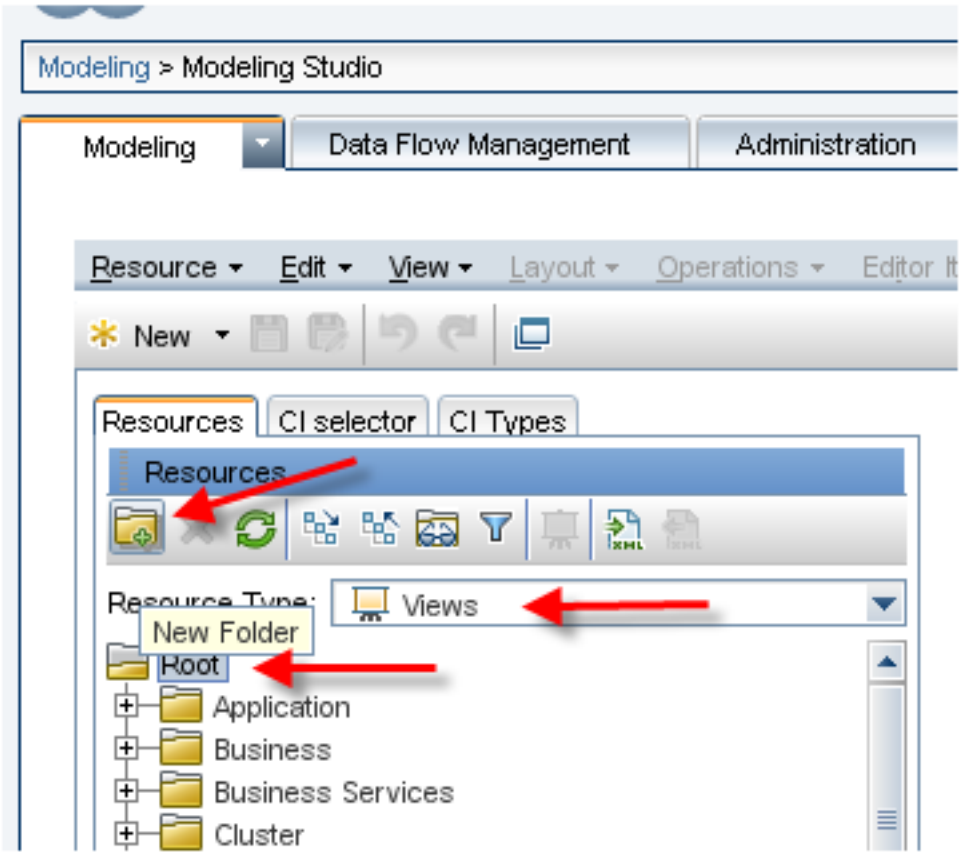
- If you prefer to do this before EUM configuration, create the Business Application in **Admin > RTSMAdministration > Modeling Studio**, and fill the **TenantOwner** attribute with the relevant value. In EUM Administration you will edit the CI and add BPM/RUM configuration.
- If you prefer to do this after EUM configuration, edit the Business Application CI's properties in **Admin > RTSM Administration > IT Universe Manager**, and fill the **TenantOwner** attribute with the relevant value. If you will use naming conventions for the Business Applications (such as using tenant name as suffix), you can easily assigning the **TenantOwner** attribute with an enrichment rule.

Once the application is configured for monitoring, you will use the Custom event template to add the **TenantOwner** attribute for automatic assignment of events to the respective event consoles (see Enriching events which are generated from within BSM).

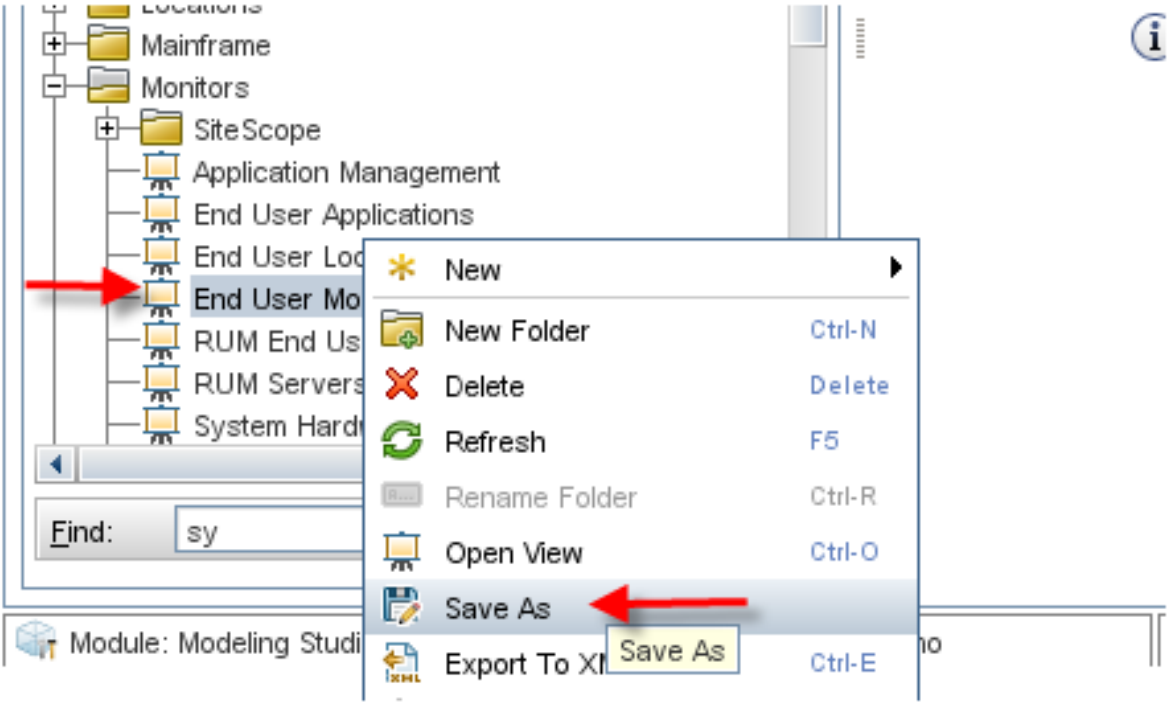
Chapter 8: Create Views in APM

Use the following procedure to create different pattern-based views for different tenants, and to add conditions to the CITs in each view to collect data relevant to the tenants. In this procedure, the **TenantOwner** attribute is used to identify and limit the data relevant to the tenants, and user level permissions are configured for the respective tenants.

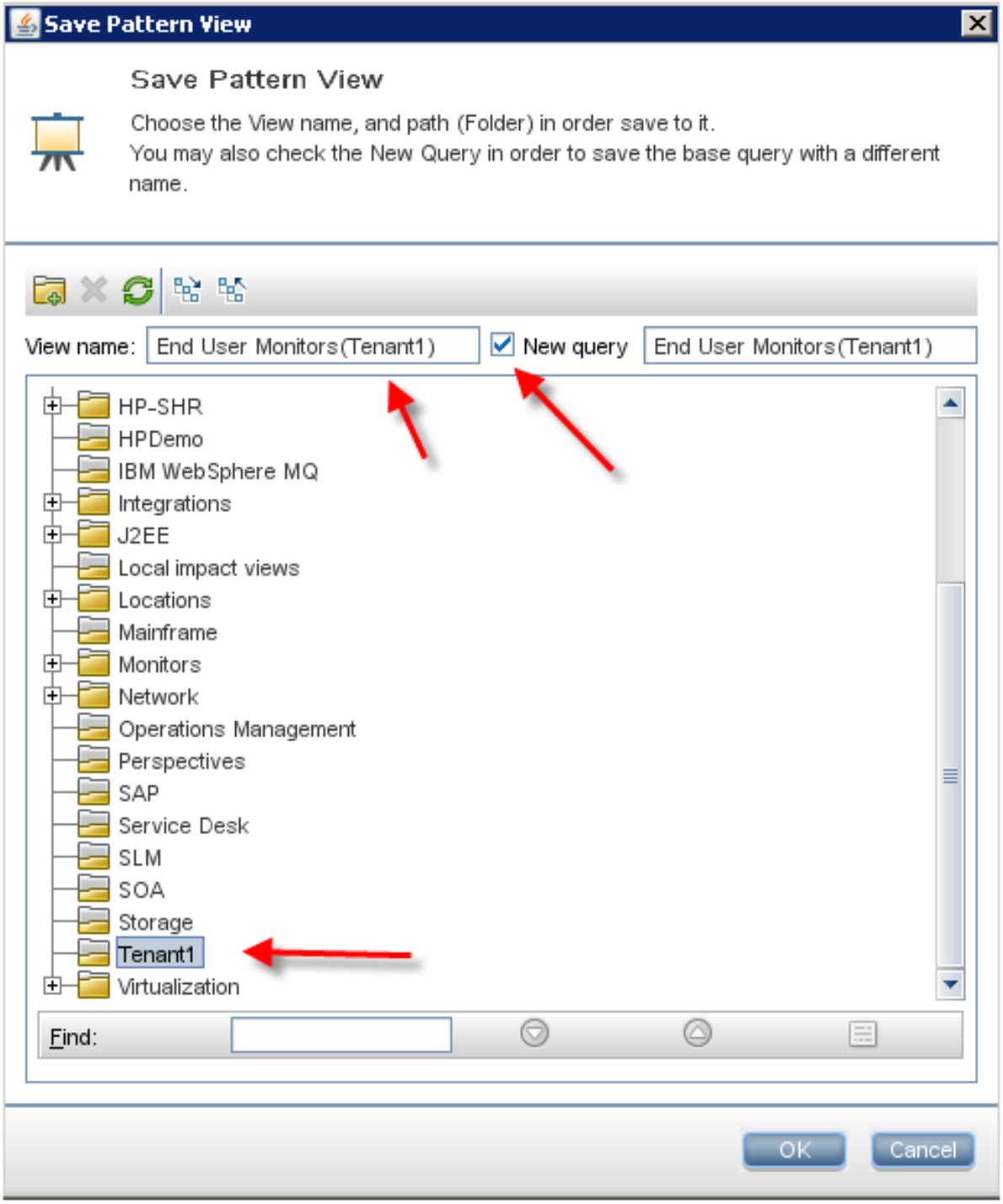
1. Within **Admin > RTSM Administration > Modeling Studio**, create a folder for each tenant. This will hold all the views belonging to that tenant and make it easy to manage the views.



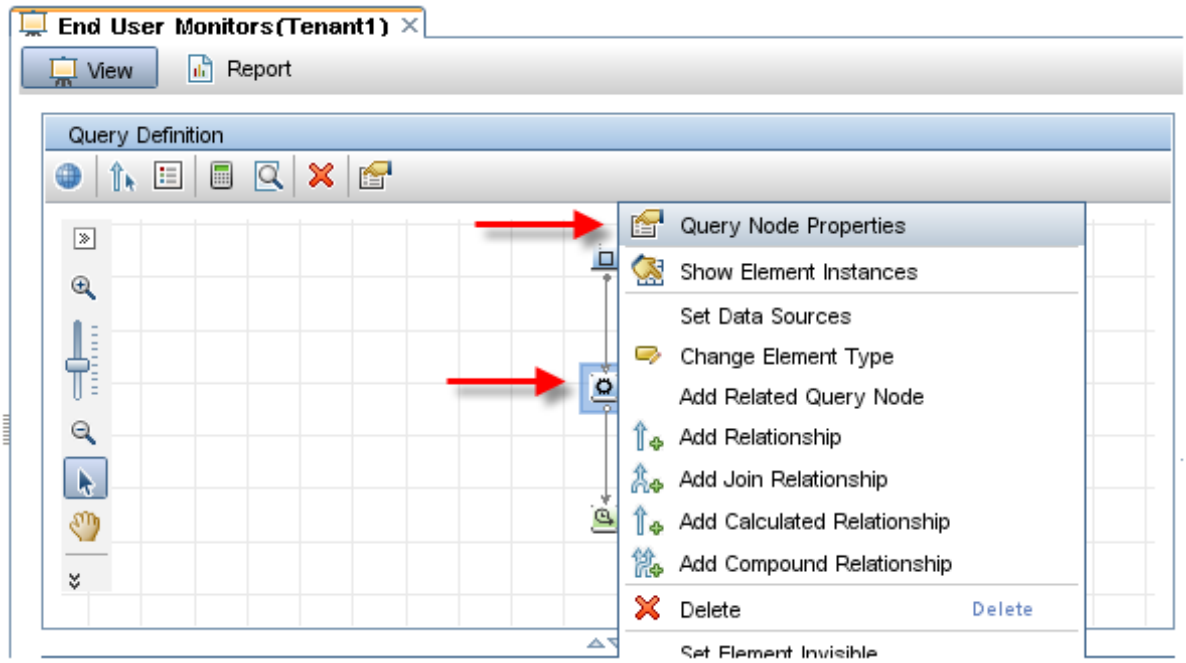
2. Right-click a view, and select **Save As** to create a view for a specific tenant.



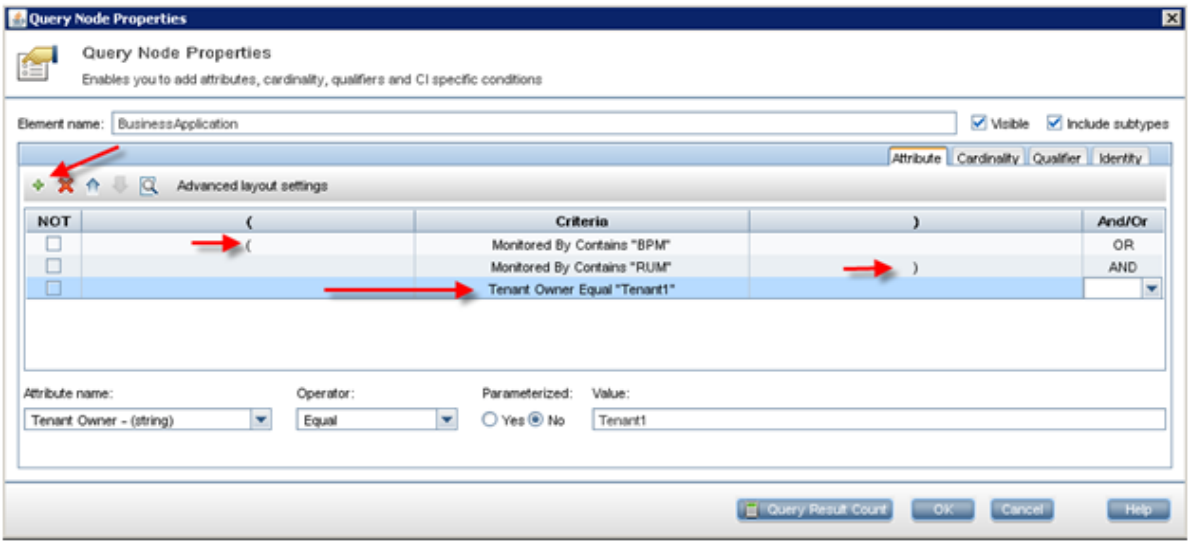
3. Give the new view a relevant name and save it in the correct folder. Make sure you select the **New query** checkbox.



4. Select the cloned view, and edit the node which will have tenant owner information for filtering. In this example, we will edit the Business Application CI (see "Configuration for End User Monitoring" on page 18):



5. Add a new property condition; select the **TenantOwner** attribute, and enter the relevant value. Do not harm the logic of the existing condition (if it exists); if necessary add parentheses to maintain the existing condition:



6. Click **OK**.
7. When you finish filtering the query nodes, click **Preview** to validate the view results.
8. When you finish validating, click **Save**.

Note: You might want to create a view which shows all the CIs that do not have the **TenantOwner** attribute defined as expected, or that are connected to such CIs. Such a view is very useful for the super-admin.

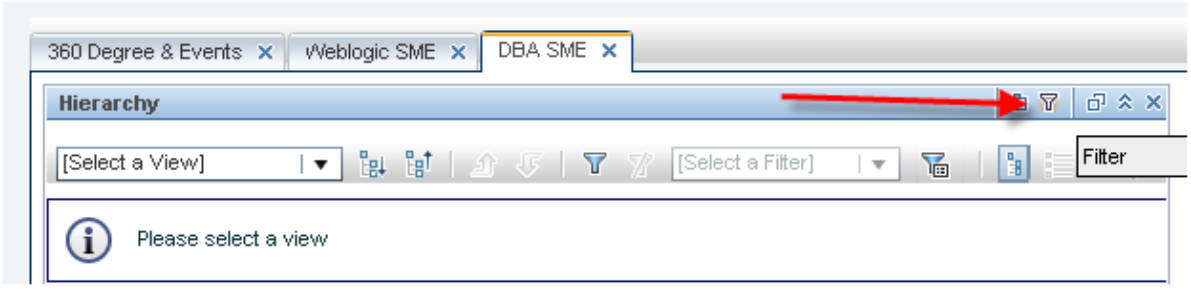
Chapter 9: Create MyBSM Pages

You can create different MyBSM pages for different tenants. These pages can be filtered to specific views in order to differentiate tenants' workflows and provide each tenant with specific Dashboards. You can also configure permissions for each page, so users will not be able to modify the pages.

Components which contain a view selector are only populated with the views that a user has permissions to access.

You can also create new URL-based components in MyBSM, for example using a tenant's knowledge base portal. You can then assign permissions for these components (see "Configure Users and Permissions" on page 24).

1. Within MyBSM, create a new page or open an existing page and save it with a new name.
2. Build your page by adding the relevant components.
3. Click **Filter** on a Service Health, SLM or EUM component.



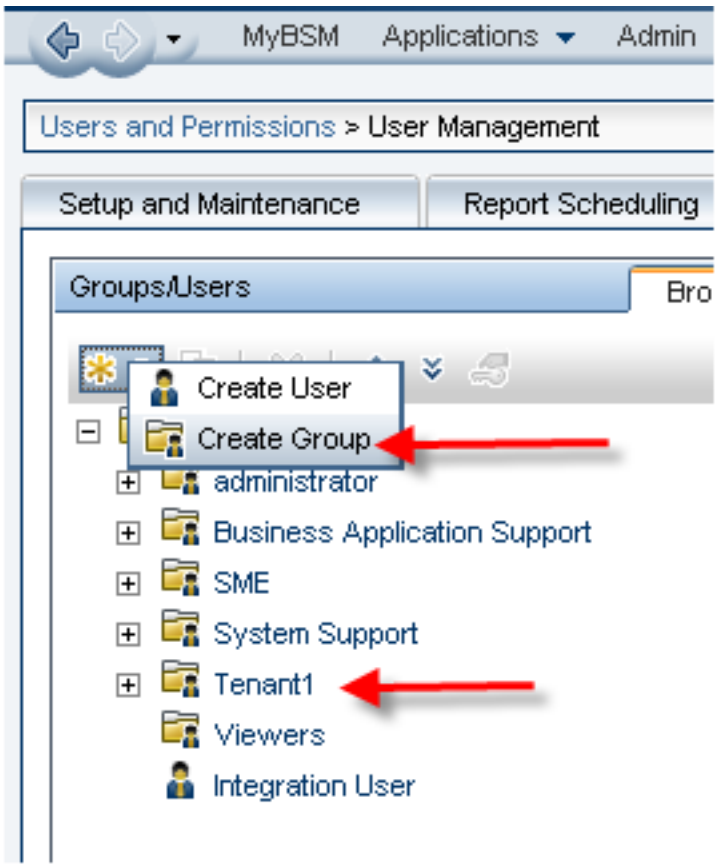
4. Select the relevant filter criteria (view, SLAs or Business Applications) and click **OK**.
5. Click **Save**.

For more information on working with MyBSM, refer to the MyBSM part of the APM User Guide.

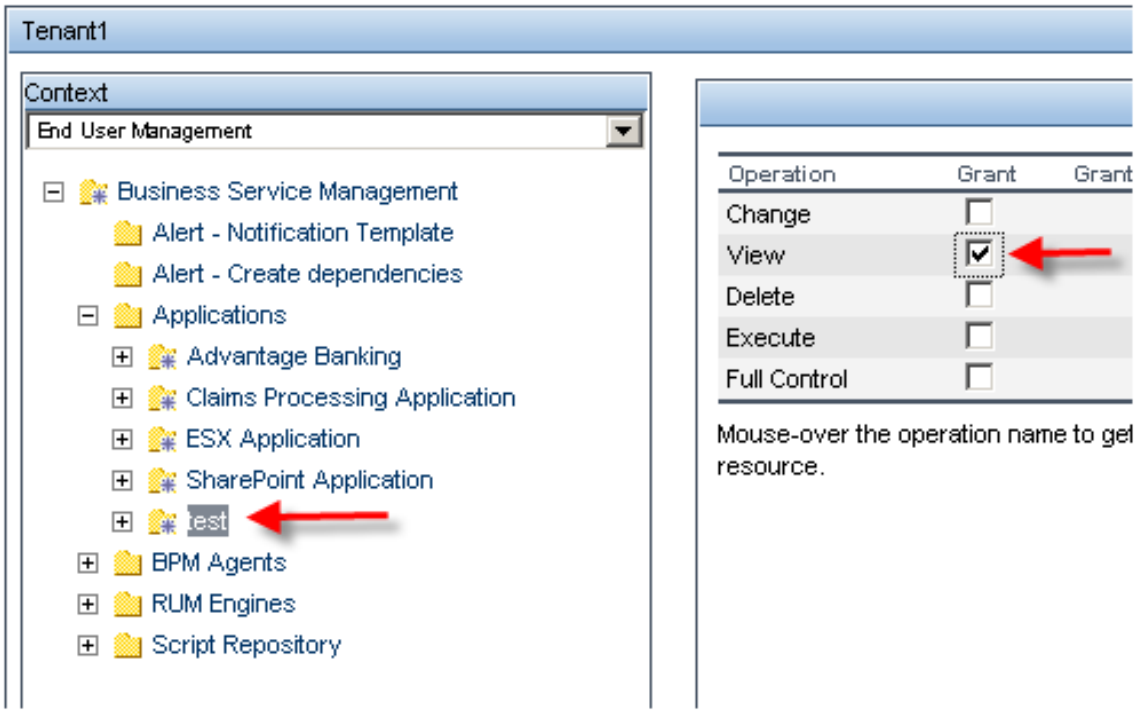
Chapter 10: Configure Users and Permissions

Use the following procedure to define group-level role-based permissions. You will use user groups to identify tenants and distinguish between users of each tenant. By defining permissions on the user group level, you avoid managing permissions on the user level. Moreover, when a new user is added to a group, it inherits permissions from the group. If a user belongs to two groups, the user gains access to events and views of two tenants.

1. Access **Admin > Platform Administration > Users and Permissions > User Management**.
2. For each tenant, create a group:



3. Edit permissions for each group you create, as follows:
   a. Select the group.
   b. Select the **Permissions** tab; click **Apply Permissions** after each modification.
   c. Select the End User Management context, and assign operations for each element (for example, you can grant View permissions for the tenant's applications only:



d. Select the **Operations Management** context. Make sure that **Events not assigned to user** is not selected, and **Events assigned to user** is selected. You can also set permissions on tools, actions and other administration tasks.

e. Select the **RTSM** context and assign View permissions to the specific views you created for this tenant. Make sure other tenants' views are not selected. You will probably want to de-select the out-of-the-box views for this tenant , they are Pattern views which are not filtered for specific tenant owner.

f. Select the **Service Health** context and assign permissions to MyBSM pages for this tenant.

g. If you created SLAs for this tenant, select the **Service Level Management** context and assign permissions for these SLAs.

h. If you create custom, trend or service reports for this tenant, select the **User Defined Reports** context and assign permissions for each category for this tenant.

For more details on users and permissions, refer to the APM Platform Administration Guide.

Chapter 11: Multi-Tenancy and Other Data Collectors

Some data collectors support multi-tenancy more easily than others:

- **BPM.** APM can handle multiple BPM agents, which means that you can have different BPM agents for different tenants. This allows fully segregation between tenants.
- **RUM.** APM can handle multiple RUM engines and each engine can handle multiple RUM probes. This allows fully segregation between tenants.
- **SiteScope.** APM can handle multiple SiteScope instances, so you can have different SiteScope instances for different tenants. Since SiteScope creates topology in RTSM, you can also use the **RoutingDomain** attribute to segregate the topology that each SiteScope creates. You can populate the **TenantOwner** attribute using enrichment, or you can use the SiteScope Profile CI in your enrichment.
- **Diagnostics.** Only one Diagnostics server/commander can be connected to APM. You can connect multiple Diagnostics probes to the server/commander, but the data and topology that are sent into APM will not have any tenant information; you must assign topology and data to specific tenants manually. You can assign permissions on the Application within User Management, in the context Transaction Management.
- **NNMi.** Only one NNMi server can be connected to APM. Future versions of NNMi will enable multi-tenancy, but currently you must manually assign the topology to tenants (or using enrichment, for example based on IP address ranges). This is also true for events with more complicated Groovy script.
- **APM Connector/IA.** APM can work with multiple connectors, which means you can have a different connector for each tenant. You can also customize topology, and include the **TenantOwner** attribute in the topology sent by the connector. You can also customize events and include the **TenantOwner** attribute in the event itself.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Multi-Tenancy Using APM - Best Practices (Application Performance Management 9.30)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Sw-doc@hpe.com.

We appreciate your feedback!