DELL Technologies

Technical White Paper

Dell EMC SRM: Multi-Tenancy Overview

Abstract

This white paper provides an overview of the multi-tenant capabilities in Dell EMC Storage Resource Manager (SRM).

September 2020

H18465

Revisions

Date	Description
September 2020	Initial release

Acknowledgments

Author: Roy Laverty

Table of contents

Executive summary

Dell EMC SRM is a market leading, comprehensive, storage monitoring and reporting solution that helps IT to visualize, analyze, and optimize their end-to-end heterogeneous storage environments. Dell EMC SRM features a role-based security model ideally suited for cloud providers, self-service IT organizations. This white paper is an introduction to the multi-tenant capabilities in SRM.

Audience

This document is intended for IT administrators, storage architects, partners, and Dell Technologies™ employees. This audience also includes any individuals who may evaluate, acquire, manage, operate, or design a Dell EMC SRM implementation,

1 Introduction

SRM is a comprehensive “on-prem” storage infrastructure monitoring and reporting solution helping IT organizations to visualize, analyze, and optimize their end-to-end heterogeneous storage environments from a single pane of glass.

SRM data collection and reporting are automated allowing you to focus on business needs and spend less time manually collecting, normalizing, and aggregated key operational metrics.

The five key use cases in SRM are workload analysis, configuration compliance, capacity planning, chargeback reporting, and performance troubleshooting.

Workload Analysis helps you decide where to place a storage workload, for the best capacity, price, and performance. Helping storage teams in identify underutilized and overutilized resources allowing them to rebalance existing workload to maintain performance and sustain their storage growth.

Configuration Compliance ensures that the customer’s environment is properly configured according to their own stack, industry best practices, and with the Dell EMC Support Matrix. It also tracks configuration changes and determines if recent changes have potentially placed data or business at risk.

Global **Capacity Planning** dashboards save you hours by eliminating manual data collection and reporting. Provide information about when additional storage will be needed. This visibility ultimately helps control storage consumption and improves ROI.

With its **Chargeback** capability, SRM tracks the true storage costs, supporting service levels, replication, and applications. This data helps storage teams communicate the value of the storage services provide to users.

Performance Troubleshooting helps you troubleshoot performance issues and identify bottlenecks.

1.1 Terminology

The following terms are used throughout this document.

Active Directory (AD): Active Directory is a directory service developed by Microsoft.

Bind: Binding is a term that is used for a user that has successfully authenticated with a directory service.

Data Enrichment: Data enrichment in SRM is creating new meta data for metrics allowing the grouping and filtering of data based on certain criteria.

Lightweight Directory Access Protocol (LDAP): LDAP is an open-source directory service.

Metric: A metric in SRM is a timestamp-value pair.

Profile: A profile in SRM defines the locale settings for a user or group of users, including time zone, default report, and authentication screen logo.

Properties: Properties in SRM are the meta data that is associated with metrics. They define the metric and enrich the data.

Realm: A Tomcat realm is a construct that allows Tomcat to authenticate users against an authentication source such as Active Directory, LDAP, or local realm.

Role-Based Access Control (RBAC): RBAC is a security model controlling user access to information based on a defined role.

Roles: Defines the rights and restrictions that are applied to a user or group of users.

SolutionPack: Installable package that provides data collection and reporting for vendor and platform-specific infrastructure components.

User: A user in SRM can be a local user or mapped to an external authoritative source such as AD or LDAP.

2 SRM Architecture

SRM natively supports multi-tenant environments, which are accomplished using the following elements:

i. Data grouping and enrichment: Give IT administrators the ability to group data based on attributes such as customer name, business unit, or location.
ii. Restrict access to grouped data using filtering: Provide a mechanism within SRM that allows IT administrators to restrict access to specific, grouped, data.
iii. Role-based access control: Implement an RBAC security model allowing for role-based management.
iv. Integration with authentication sources: Allow for a flexible integration with directory services in use in most businesses.

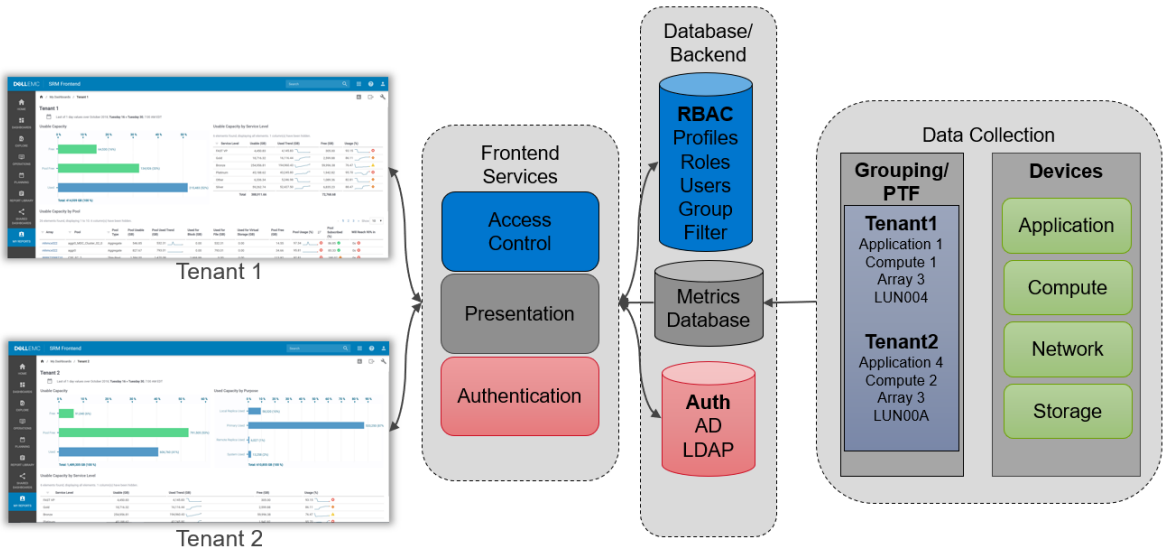

Figure 1

3 SRM Data Model

The SRM data model consists of time-series data and properties. Custom properties can also be created to enrich the data. Filtering on properties enables SRM administrators to secure and limit access to data.

3.1 Time-Series Database

SRM uses a time-series database (TSDB) model, which is designed to handle large amounts of data that are collected at regular intervals. The database schema is simple in that the time-value pair is stored in multiple tables, and the metadata are stored in a separate table. The following figure shows the relationships between the various tables in the SRM backend database.

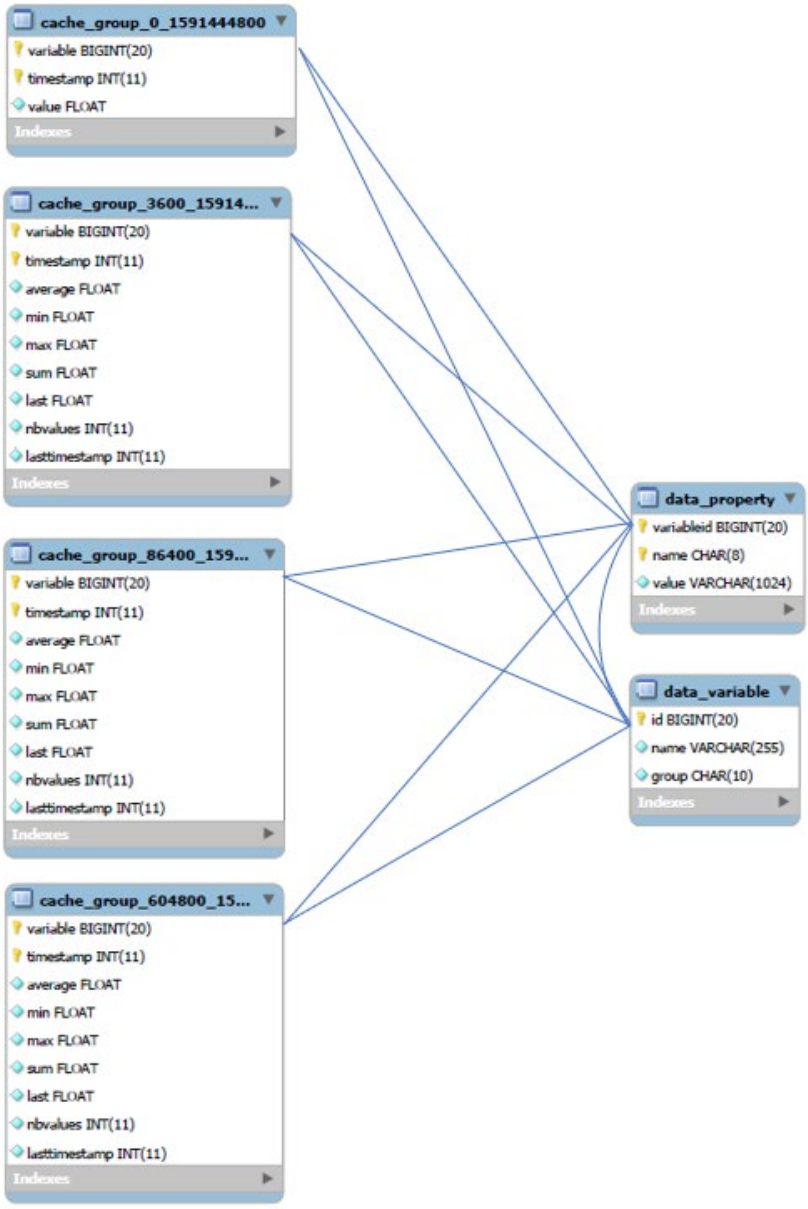

Figure 2

3.2 Metrics

The real-time values are stored in the cache_group_0_<*timestamp*> tables and contain the raw data that various collectors gather. The real-time collection intervals are defined when the SolutionPacks are installed. The backend service creates the hourly, daily, and weekly aggregations.

Table name	Period	Aggregates
cache_group_0_<timestamp>	Real-time	N/A
cache_group_3600_<timestamp>	Hourly	average, min, max, sum, last, nbvalues, lasttimestamp
cache_group_86400_<timestamp>	Daily	average, min, max, sum, last, nbvalues, lasttimestamp
cache_group_604800_<timestamp>	Weekly	average, min, max, sum, last, nbvalues, lasttimestamp

Table 1

The following example shows a real-time time-series table consisting of a variable id, timestamp, and a value.

```
mysql> select * from cache_group_0_1497895200 where variable=9732;
+----------+------------+---------+
| variable | timestamp  | value   |
+----------+------------+---------+
|     9732 | 1497895200 | 5.93597 |
|     9732 | 1497895500 |  5.9406 |
|     9732 | 1497895800 | 6.08698 |
|     9732 | 1497896100 | 7.42121 |
|     9732 | 1497896400 | 6.11345 |
|     9732 | 1497896700 | 7.00097 |
|     9732 | 1497897000 | 6.89263 |
|     9732 | 1497897300 | 6.18767 |
|     9732 | 1497897600 | 6.85586 |
|     9732 | 1497897900 | 7.22569 |
|     9732 | 1497898200 | 6.41641 |
|     9732 | 1497898500 | 6.65969 |
|     9732 | 1497898800 | 5.95368 |
|     9732 | 1497899100 | 7.47907 |
+----------+------------+---------+
```

Figure 3

The following example shows an hourly cache group. Note the various aggregates that are available in the hourly cache group which are not available in the real-time cache group.

```
mysql> select * from cache_group_3600_1498046400 where variable=9732;
+----------+------------+---------+---------+---------+---------+---------+----------+---------------+
| variable | timestamp  | average | min     | max     | sum     | last    | nbvalues | lasttimestamp |
+----------+------------+---------+---------+---------+---------+---------+----------+---------------+
|     9732 | 1498046400 | 6.23358 |  6.0753 | 6.61541 | 74.8029 | 6.18746 |       12 |    1498049700 |
|     9732 | 1498050000 |  6.2259 |  6.0505 | 6.65654 | 74.7108 | 6.16177 |       12 |    1498053300 |
|     9732 | 1498053600 | 6.41495 | 6.00387 | 7.30578 | 76.9794 | 6.33532 |       12 |    1498056900 |
|     9732 | 1498057200 | 6.18884 | 6.07368 | 6.38676 | 74.2661 | 6.13983 |       12 |    1498060500 |
|     9732 | 1498060800 | 6.09267 | 6.00504 | 6.15888 |  73.112 | 6.10816 |       12 |    1498064100 |
|     9732 | 1498064400 | 6.13321 | 5.97893 | 6.34763 | 73.5985 | 6.34763 |       12 |    1498067700 |
|     9732 | 1498068000 | 5.86772 | 4.22963 | 7.27483 | 70.4127 | 6.10727 |       12 |    1498071300 |
|     9732 | 1498071600 | 6.04535 | 5.81766 | 6.87188 | 72.5442 | 5.99069 |       12 |    1498074900 |
|     9732 | 1498075200 | 6.03002 | 5.91429 | 6.13985 | 72.3603 | 6.08277 |       12 |    1498078500 |
+----------+------------+---------+---------+---------+---------+---------+----------+---------------+
```

Figure 4

3.3 Data Properties

The properties in the *data_property* table provide context and describe the metrics that SRM collects. For example, the value of the *unit* property contains the unit of measure for the metric it is associated with. If the metric is Response Time for a VMAX Storage Pool, then the unit property is *millisecond*. A small set of properties is common to most metrics. These include source, device, devtype, part, parttype, name, and unit.

variableid	name	value
9732	arraytyp	Symmetrix
9732	bunit	Default
9732	customer	Default
9732	datagrp	VMAX-ThinPool
9732	datasrc	UNIVMAX
9732	datatype	Block
9732	devdesc	5876.285.194 date:05.21.2015 patch_date:05.21.2015
9732	device	000198700604
9732	devtype	Array
9732	dgstype	Thin
9732	isdare	false
9732	location	AMER
9732	model	VMAX10K
9732	name	ResponseTime
9732	part	FC_RAID5
9732	parttype	Storage Pool
9732	pltfmgrp	All Storage Systems/EMC VMAX|All Storage Systems|
9732	serialnb	000198700604
9732	source	VMAX-Collector
9732	sstype	Block
9732	unit	ms
9732	vendor	EMC Corporation
9732	vmaxtype	VMAX2
9732	vstatus	active
9732	w4ncert	1.0

Figure 5

To provide context around the metrics, use the variable id to join the cache group table with the data_property table, as shown in the following figure.

```
select c.timestamp,c.value,d.name,d.value from cache_group_0_1594231200 c
inner join data_property d on c.variable=d.variableid and c.variable=61217
and c.timestamp=1594231200;
```

timestamp	value	name	value
1594231200	19.2729	arraytyp	Symmetrix
1594231200	19.2729	bunit	Default
1594231200	19.2729	bwlimit	N/A
1594231200	19.2729	collhost	[redacted]
1594231200	19.2729	collinst	emc-vmax
1594231200	19.2729	customer	Default
1594231200	19.2729	datagrp	VMAX-StorageGroup
1594231200	19.2729	datasrc	UNIVMAX
1594231200	19.2729	datatype	Block
1594231200	19.2729	devdesc	5876.309.401 date:01.04.2018 patch_date:01...
1594231200	19.2729	device	000195700949
1594231200	19.2729	devtype	Array
1594231200	19.2729	inmvsg	1
1594231200	19.2729	iolimit	N/A
1594231200	19.2729	iolmstat	None
1594231200	19.2729	isdare	false
1594231200	19.2729	model	VMAX40K
1594231200	19.2729	name	AverageIOSize
1594231200	19.2729	part	EcoSys_SB_DataStore1_500gb
1594231200	19.2729	parttype	Storage Group
1594231200	19.2729	pltfmgrp	All Storage Systems/Dell EMC VMAX|All Storage ...
1594231200	19.2729	polname	N/A
1594231200	19.2729	poltype	N/A
1594231200	19.2729	serialnb	000195700949
1594231200	19.2729	sgname	EcoSys_SB_DataStore1_500gb
1594231200	19.2729	slobase	N/A
1594231200	19.2729	sloname	N/A
1594231200	19.2729	slosrp	N/A
1594231200	19.2729	slowrkld	N/A
1594231200	19.2729	source	VMAX-Collector
1594231200	19.2729	sstype	Block
1594231200	19.2729	tiertype	N/A
1594231200	19.2729	unit	KB
1594231200	19.2729	univmxip	[redacted]
1594231200	19.2729	vendor	Dell EMC
1594231200	19.2729	vmaxtype	VMAX2

Figure 6

3.4 Data Enrichment

Data enrichment in SRM is the mechanism by which new properties and values can be created. The new properties and values are created at time of collection using a Property-Tagging-Filter (PTF). The PTF contains a set of keys, properties, and values. When a metric is collected, and it has properties that match a key, new properties and values are added to the data by the PTF.

Example, when a metric with a device property of Array1 is collected a new property called location is added and the value is set to Lab 3.

Key (device name)	Property	Value
Array1	location	Lab 3
Array2	location	Lab 1
FCSW1	admin	Jane Doe
FCSW2	assetid	32178

Table 2

3.4.1 Group Management

The Groups Management UI simplifies the task of data enrichment with preconfigured properties and a simplified user interface. Some of the preconfigured properties include Location, Customer, and Business Unit.

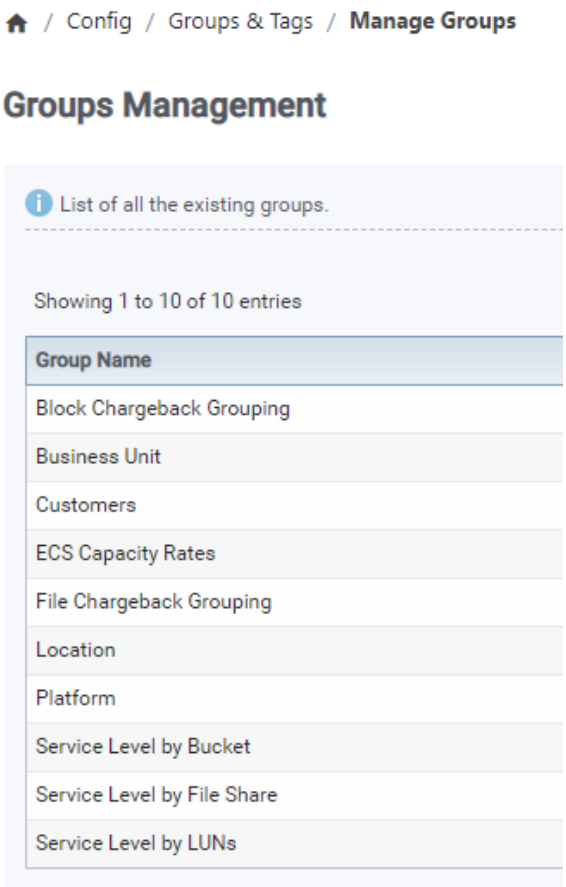

Figure 7

The following example of a **customer** group the customer property value is set to **Tenant A** when a metric is collected with a device property value of 000197600191, a parttype of LUN, and part of 0000A.

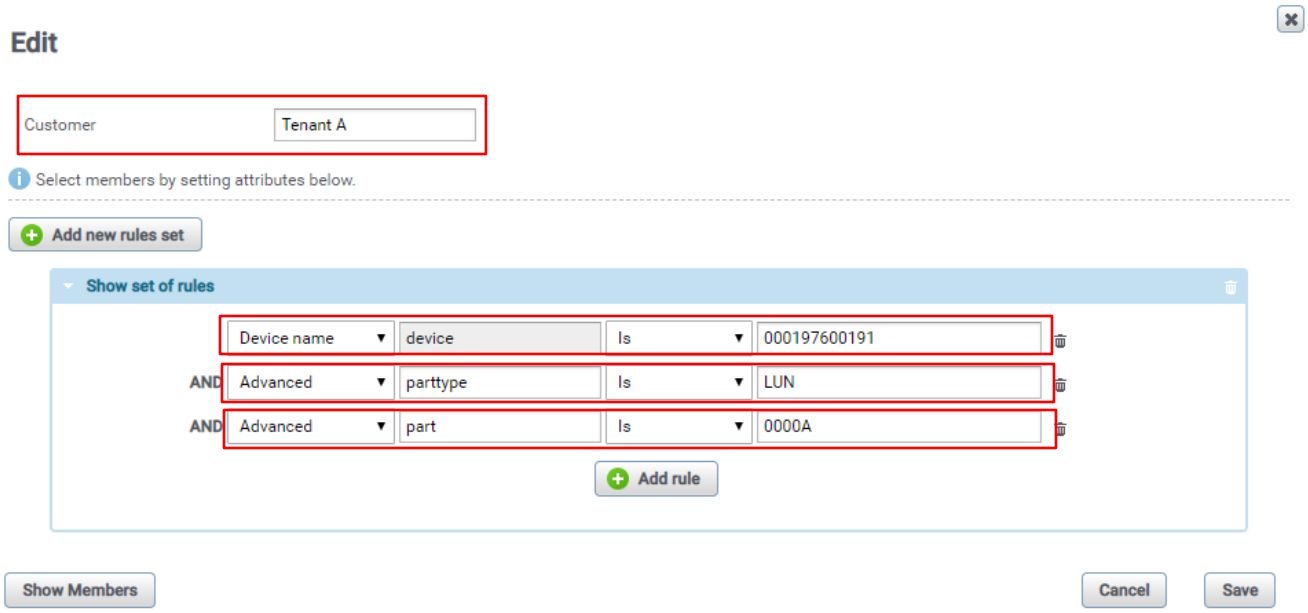

Figure 8

3.5 Filtering

Filtering is used to refine or restrict access to data in SRM. As shown in the following figure, filtering can target metrics based on a common set of properties. For example, multi-tenant environments can group data by a tenant name. Filtering is then used to restrict access to the grouped data for the tenant.

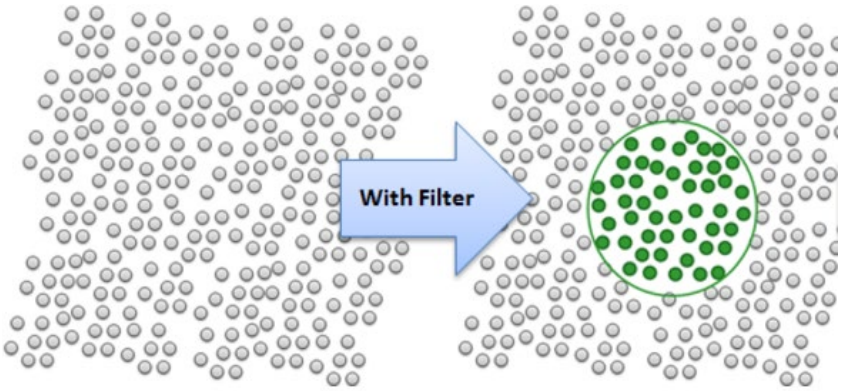

Figure 9

Example:

```
Filter=device=='000197600191'&parttype=='LUN'&part=='0000A'
```

4 Role-based access control

SRM uses a role-based access control (RBAC) authorization and access management model to restrict users to only the information they need. It can integrate with corporate Active Directory or LDAP services to authenticate and regulate access to SRM data.

4.1 Roles

SRM has six preconfigured roles, but custom roles can also be created as needed.

Name	Description
Datacenter Administrator Users	• Read Only Access to data center reports
Full Control Users	• Full read/write access to all reports • Limited access to SRM Admin UI functions
Network Administrator Users	• Read Only Access to data center reports • Limited access to SRM Admin UI functions
NOC Operator	• Read Only Access to all reports for network operations center (NOC) operators
Storage Administrator Users	• Full read/write access to all reports • Limited access to SRM Admin UI functions
Web Service Role	• Used for web service calls only

Table 3

A role consists of a filter, members, external members, template access, actions, and module access. The role's filter is used to restrict access to the wanted grouped data. All users that are configured with this role only have access to data that is specified in the role's filter. The single exception is if a user is assigned multiple roles. When a user is assigned to multiple roles, filters from all assigned roles are combined using an OR function.

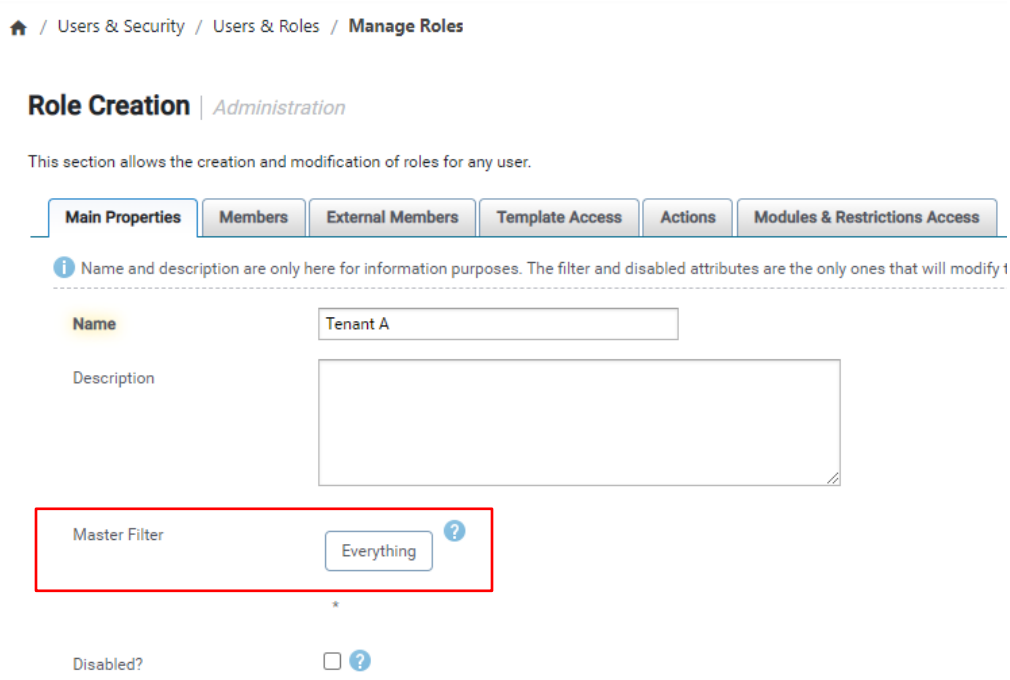

Figure 10

Members of a role can be internal user-defined in SRM or external users that belong to a group in a directory service. External groups are bound to an SRM role using standard distinguished name format as seen in the example in Figure 11.

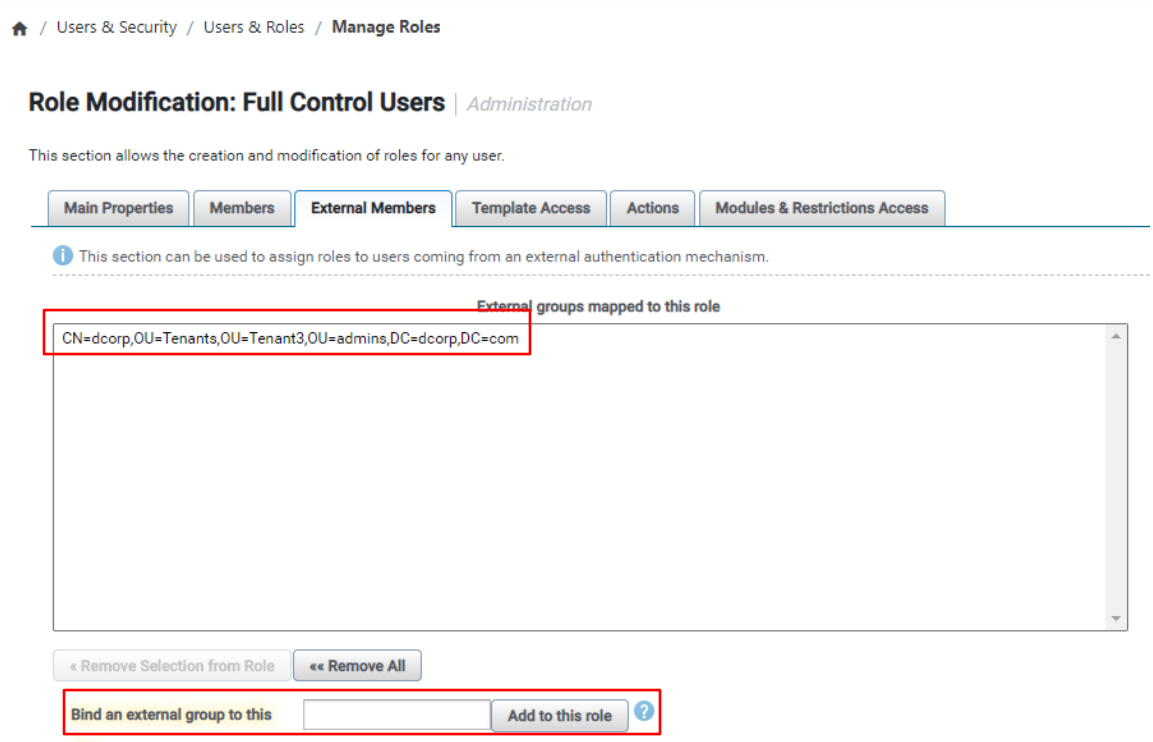

Figure 11

Access to standard SolutionPack reports can be defined globally, at the SolutionPack level, and at individual report template level. Rights are evaluated starting with the individual report template, then the SolutionPack level, and finally at the global level.

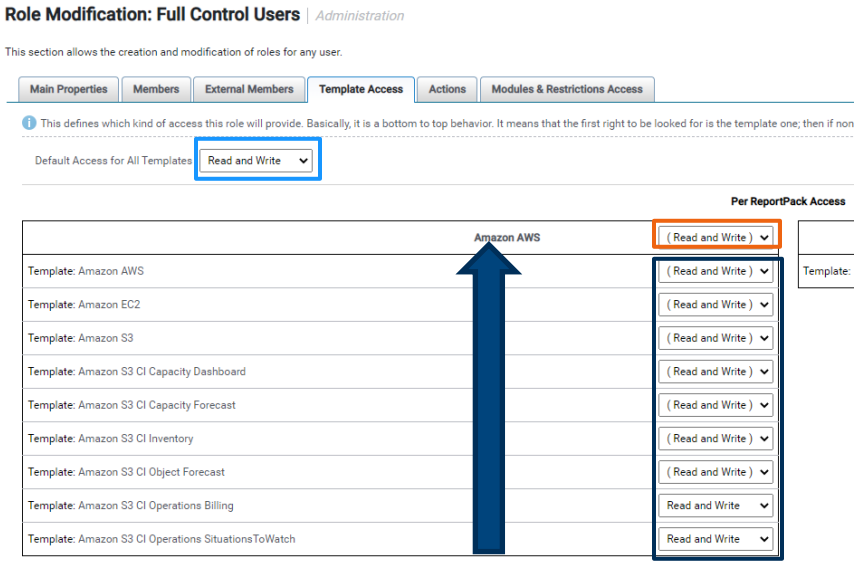

Figure 12

SRM has a few user actionable functions in the reporting interface. The two most common actions relate to alert management and managing what-if scenarios. Restricting SRM users' access to actions is performed at the role level. The actions can be assigned individually or inherited from a parent role if configured.

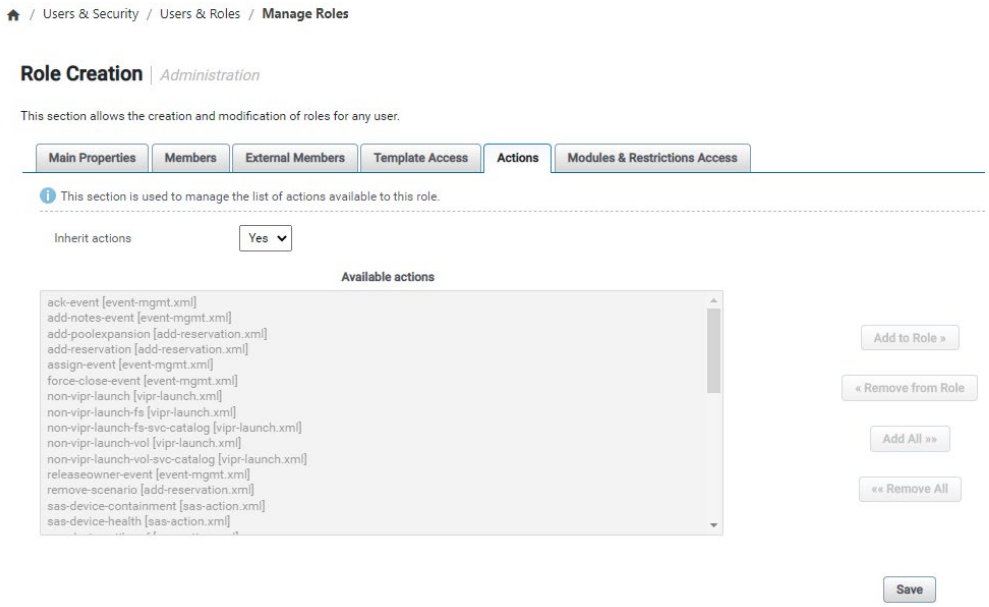

Figure 13

A role is used to provide or restrict access to various SRM modules including the user interface, administration UI, or alert configuration management. Module access can be inherited from the parent role or enforced. The UI, Alerting, and Centralized Management modules offer the ability to limit access to module features. For example, a role that allows access to the SRM UI can be configured to restrict access to the report editor.

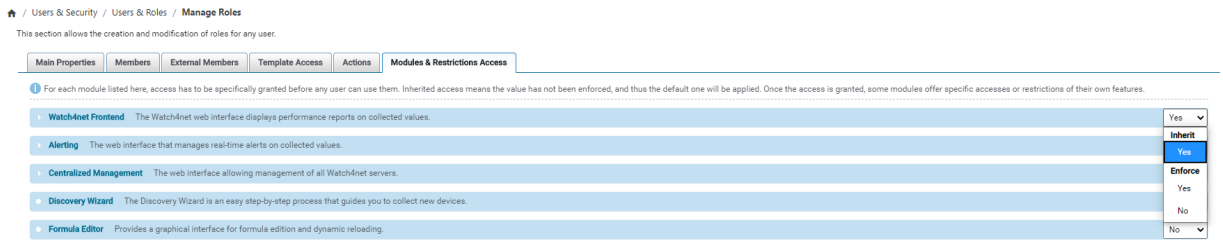

Figure 14

4.2 Users

A user account can be configured as a Global Administrator, Normal User, or External User. A global administrator account cannot be disabled. A normal user account is the default status for newly created users and can be disabled. An external user is one mapped to external authentication source. An external user can only be disabled at the role level.

Each user has a master filter, which is combined with user's role filter using an AND function.

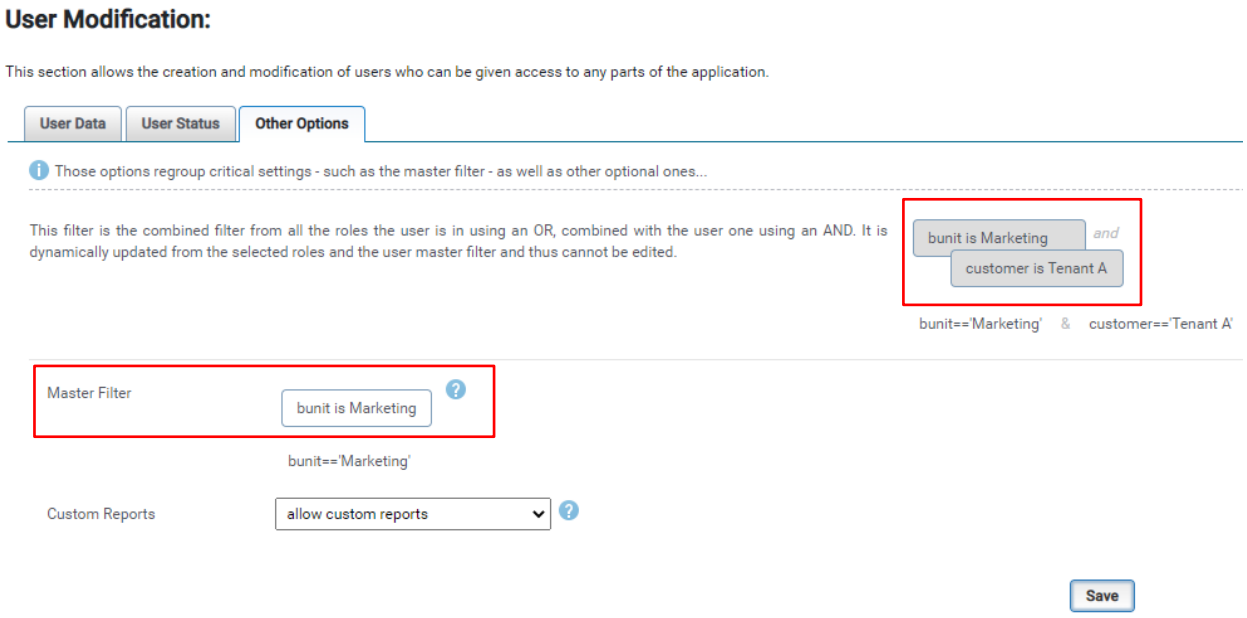

Figure 15

4.3 Profiles

Profiles are used to customize the end-user experience. Profiles contain settings including logo, locale, report auto refresh rate, and login report. A profile can be mapped to an external group as well.

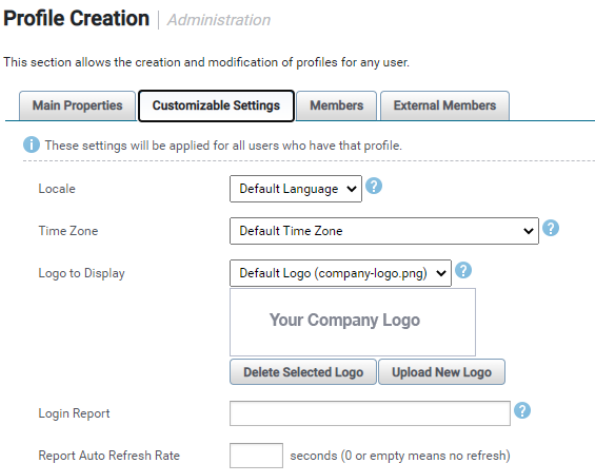

Figure 16

5 Authentication

Authentication in SRM is managed using realms, which are resources that represent authentication sources. The default realm in SRM is a local database on the primary backend virtual machine. SRM supports multiple types of authentication sources such as Active Directory and LDAP.

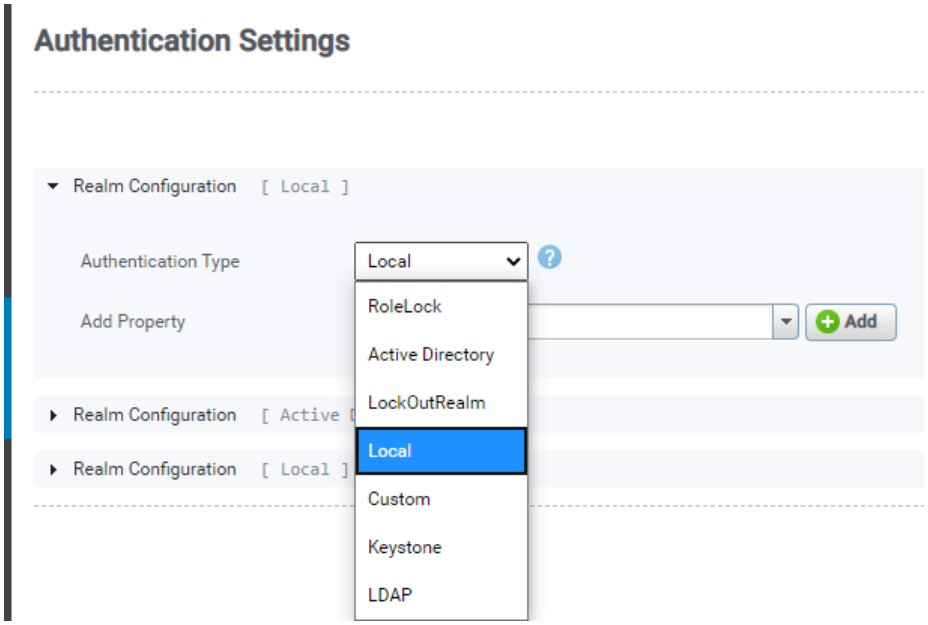

Figure 17

6 Chargeback Example

A common multi-tenant use case is providing storage consumption and costs for a tenant. Chargeback is a key use case in SRM and when combined with multi-tenancy functionality allows storage administrators to automate reporting for their customers. This example provides an overview of the process of enriching the data and granting read-only access to the tenant user to chargeback data.

6.1 Data Enrichment

The tenants are defined in the customers group, which is added to the block chargeback group. Cascading groups in this manner allows us to take advantage of the customer grouping for RBAC purposes. The block chargeback group allows the customer to review their storage consumption and costs in the chargeback reports.

We create a customer group called *Tenant ABC* and assign it the virtual machine that this tenant is consuming as seen in Figure 18.

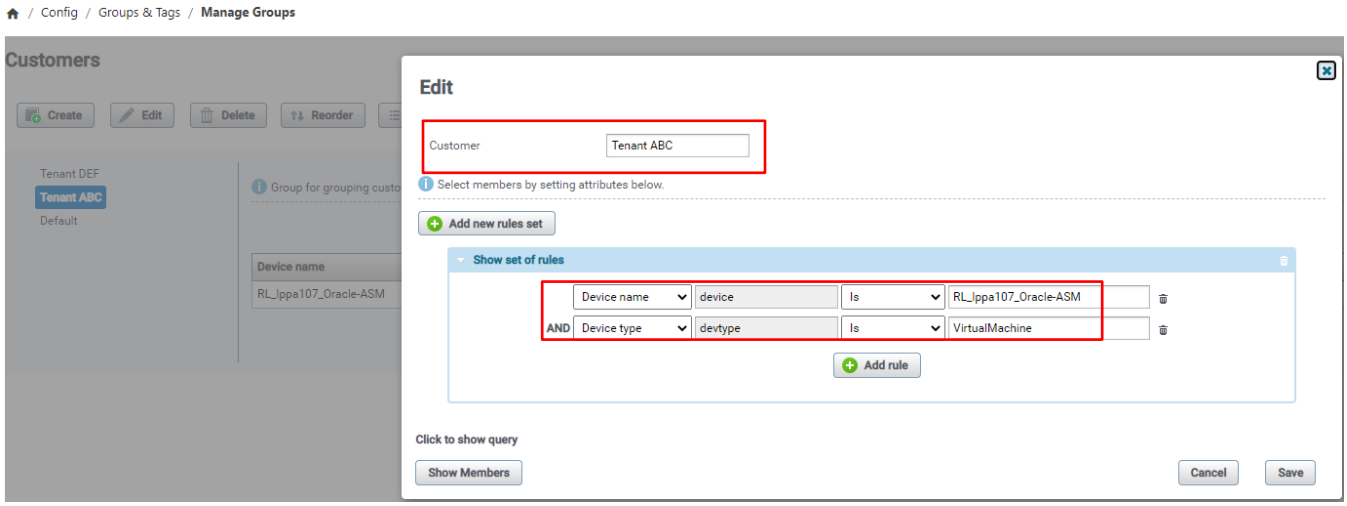

Figure 18

We create a block chargeback group of the same name. The rule for the block chargeback group uses the customer property that was created in the previous step (Figure 19).

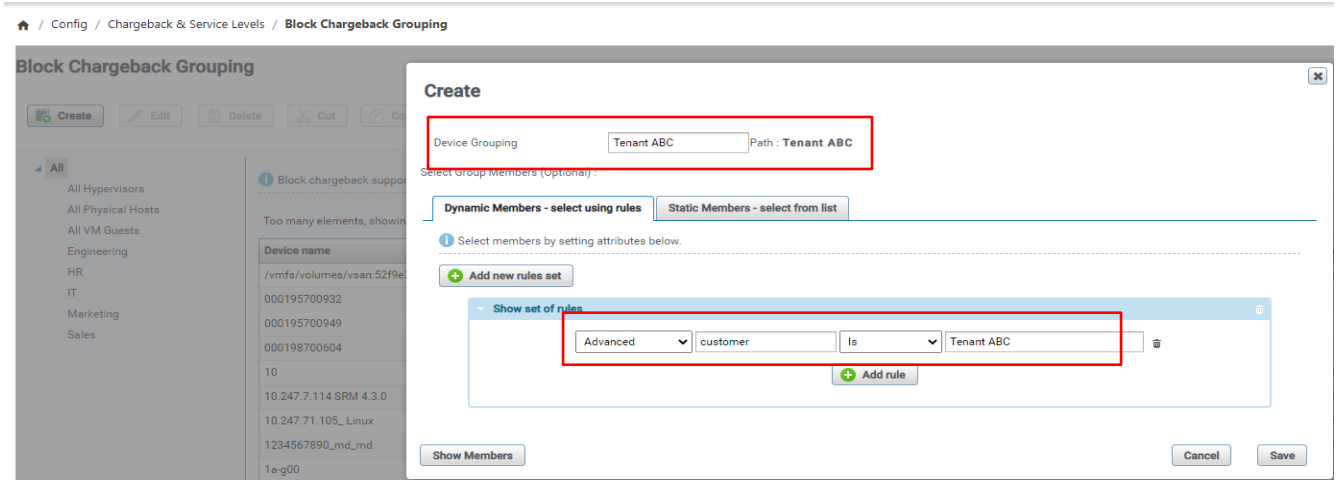

Figure 19

6.2 Roles and Profiles

For this use case, we start by creating a read-only role for our tenant. We name the role *Tenant ABC* and set the Master Filter to *customer is Tenant ABC* as seen in figure 20.

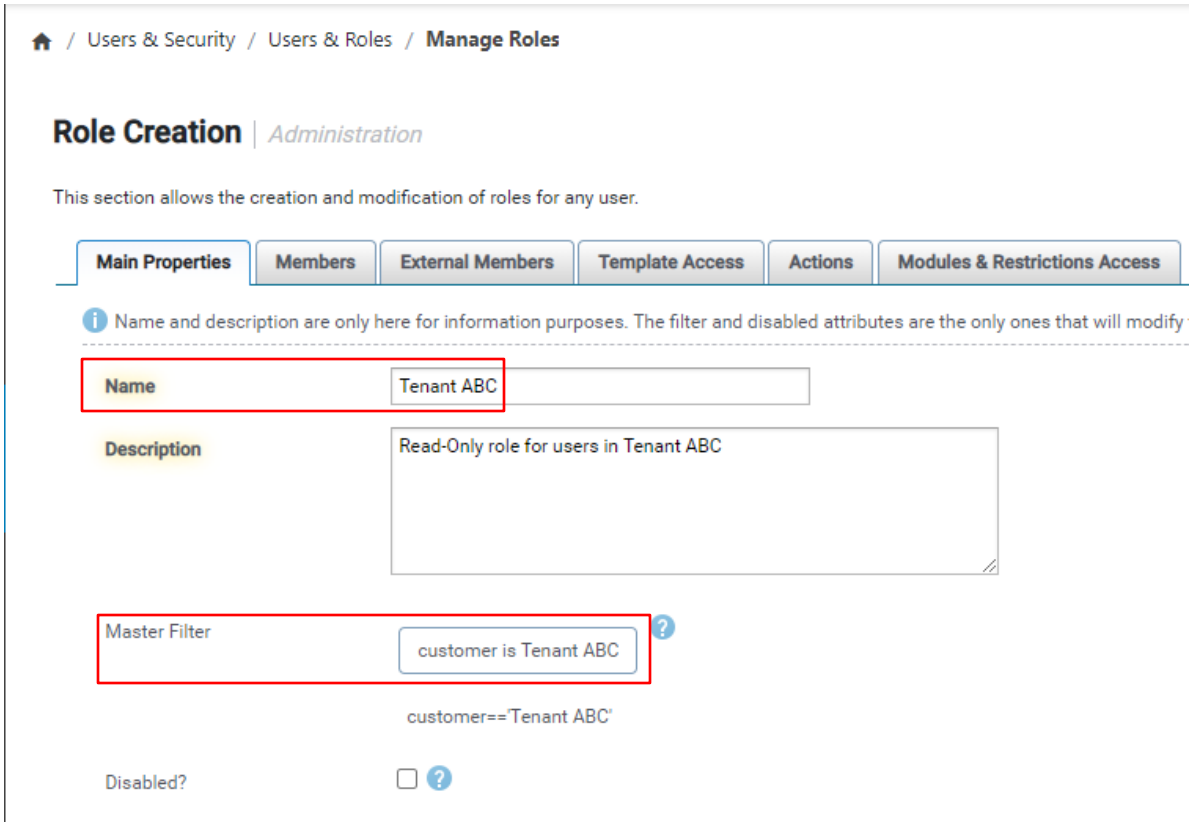

Figure 20

For our use case SRM is configured to use an active directory service. We use the External Members tab to bind *Tenant ABC* users AD group to our role.

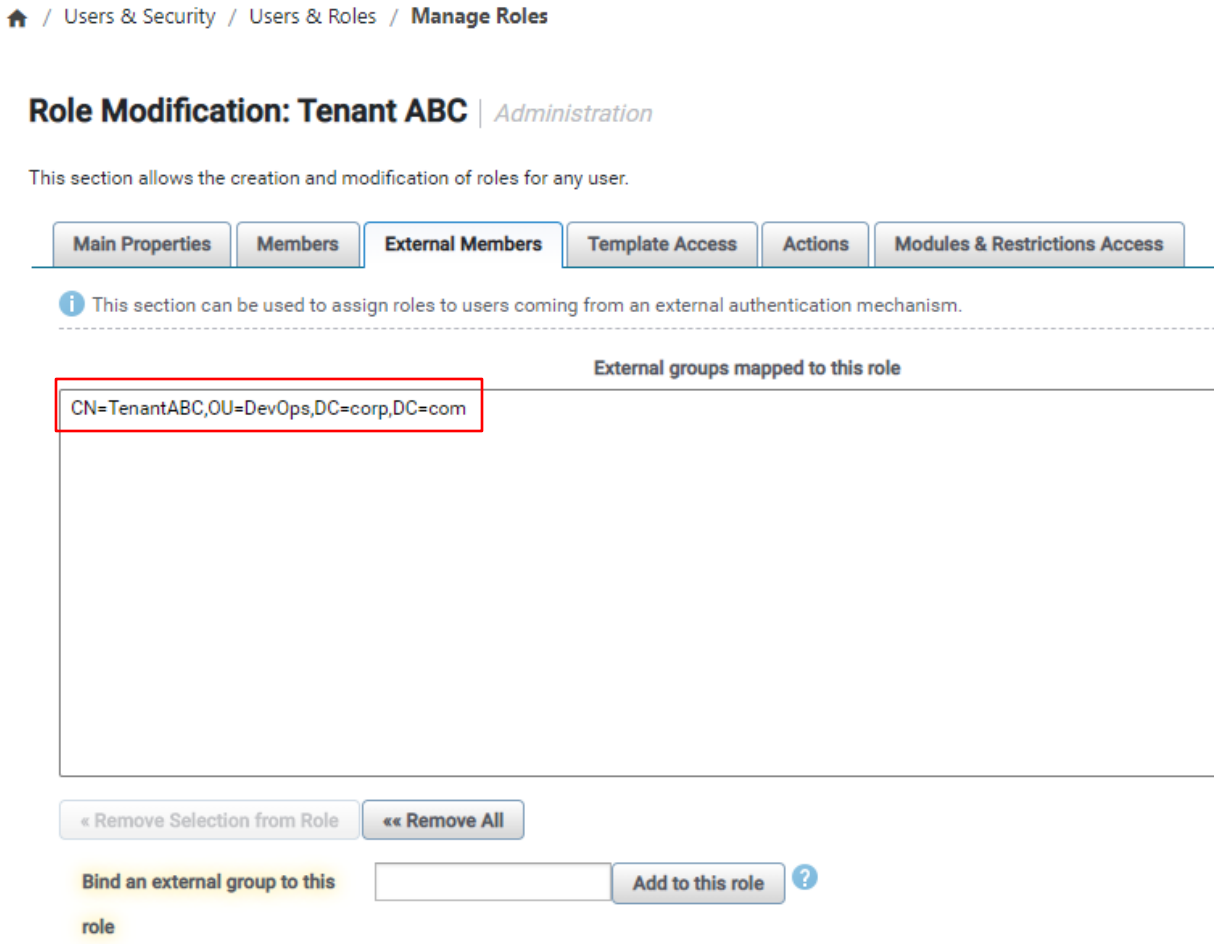

Figure 21

On the Template Access tab of the role, we set the Block Chargeback to Read-Only. We also need to set the Operations tab under the Default ReportPack to Read-Only because the chargeback reports are located under the Operations menu.

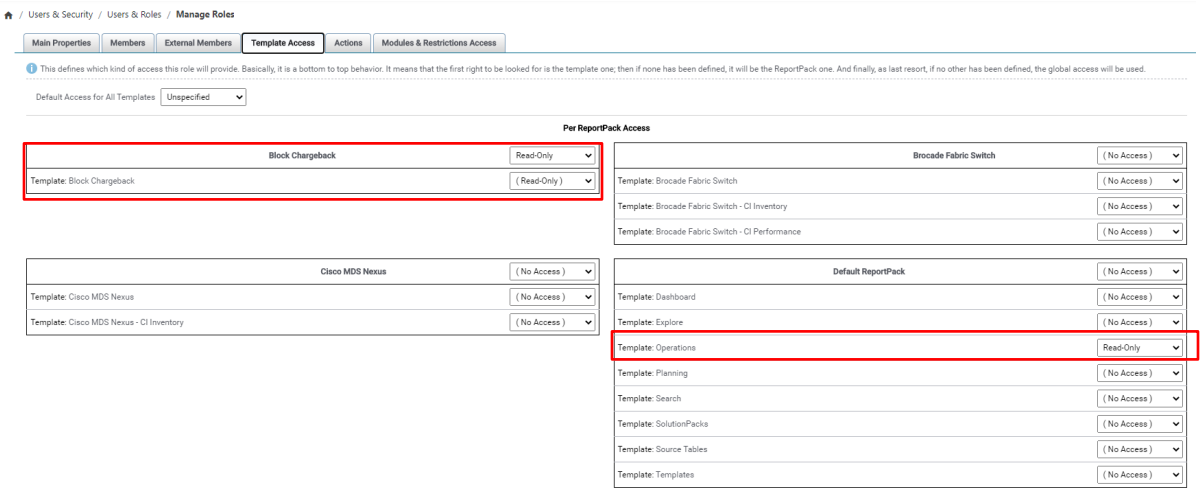

Figure 22

Module access can be limited to frontend only to allow the tenant to view the chargeback report.

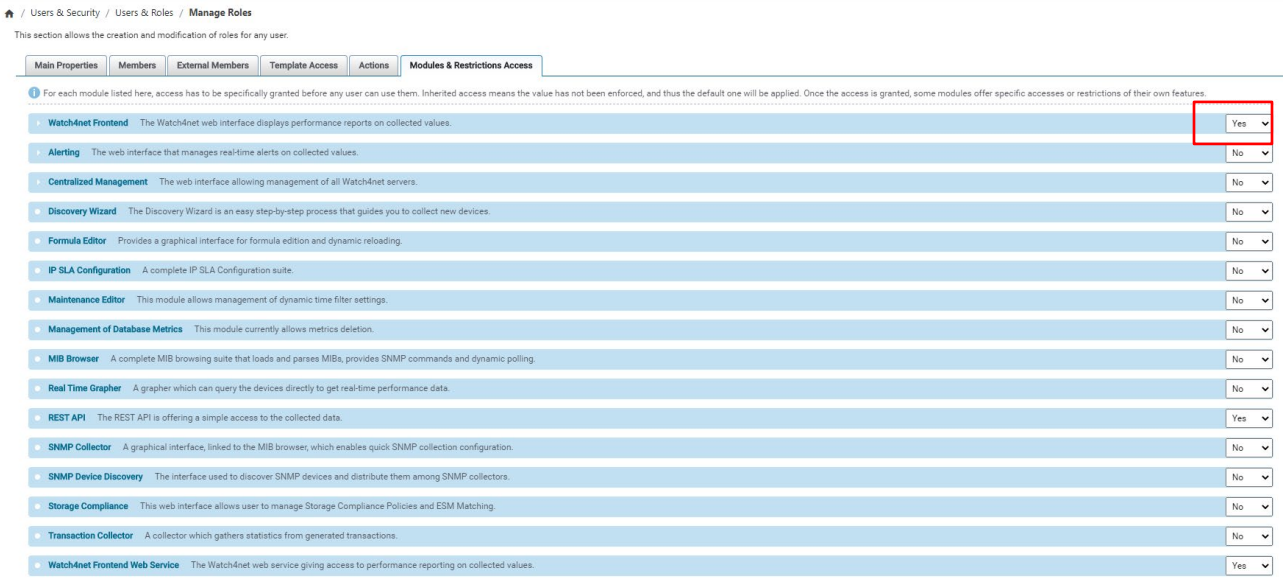

Figure 23

For this use case, the tenant needs a custom profile primarily to define the login report.

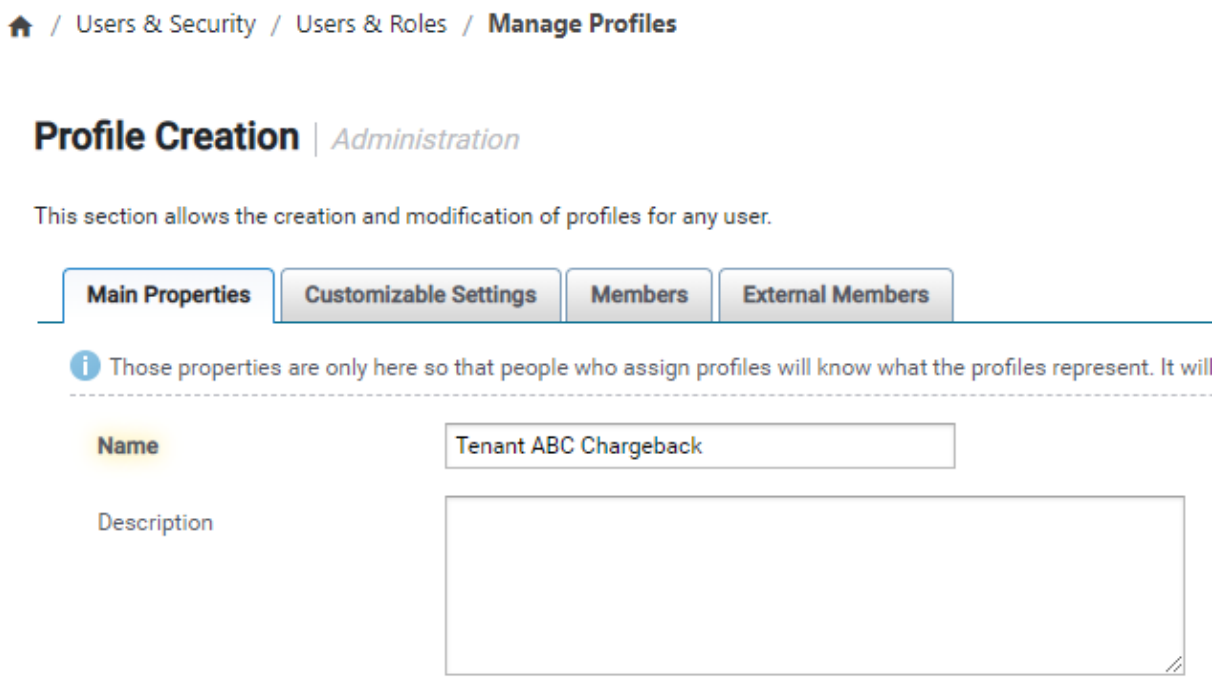

Figure 24

On the Customizable Settings tab. We set the logo to be displayed at login. The login report field allows the SRM administrator to specify the location of the report that appears at login. The user will see the default dashboard when they log in if this field is left blank. In this example, we want the *Tenant ABC* users to see the Chargeback by Virtual Machine report.

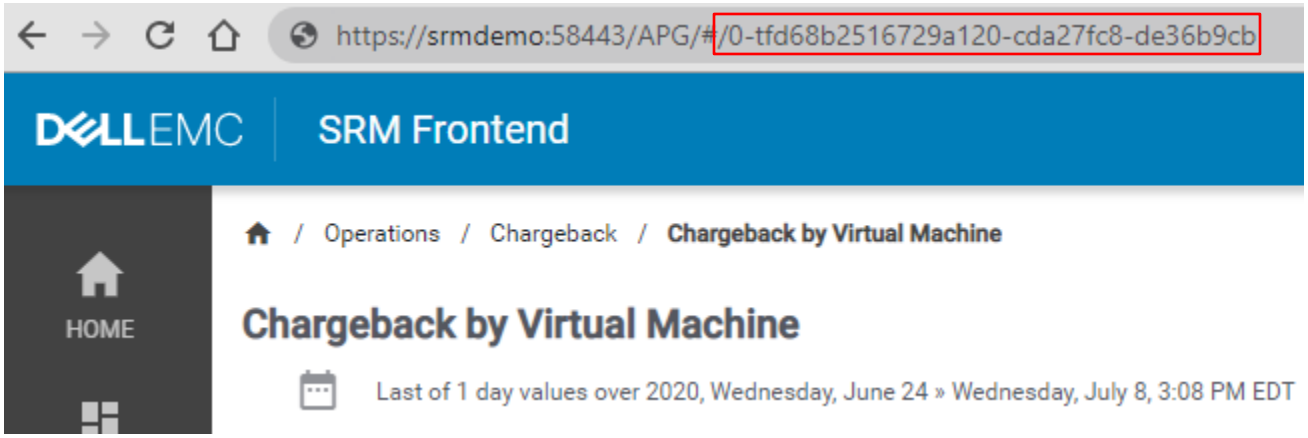

Figure 25

Here we set the login report to the Chargeback by Virtual Machine report.

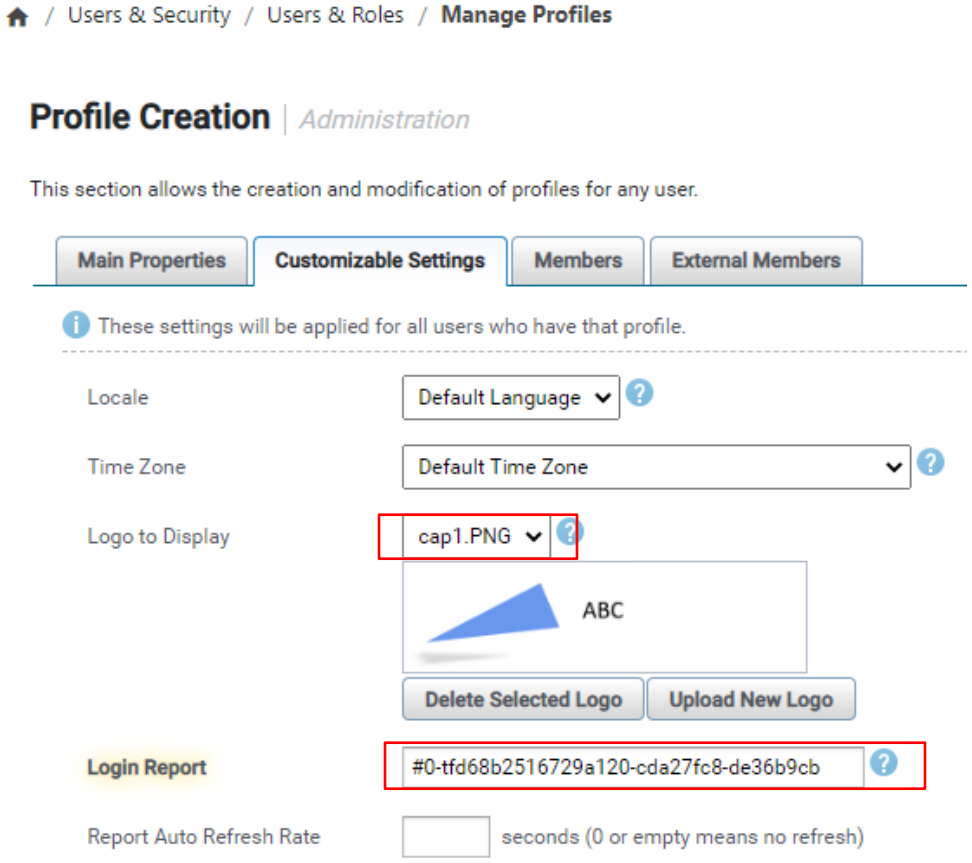

Figure 26

As we did with role configuration, we map our *Tenant ABC* AD group to the profile.

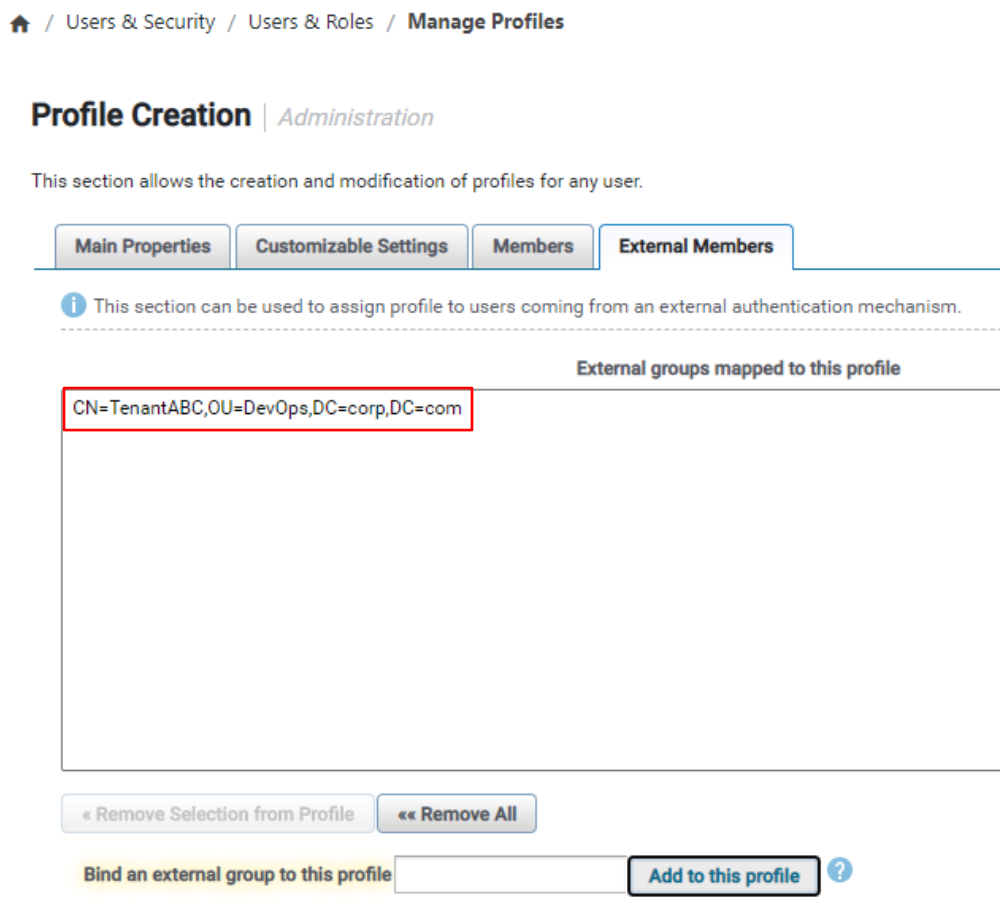

Figure 27

A user from *Tenant ABC* has read-only access to the Chargeback by Virtual Machine report and can only view data that has been grouped in their tenant (Figure 28).

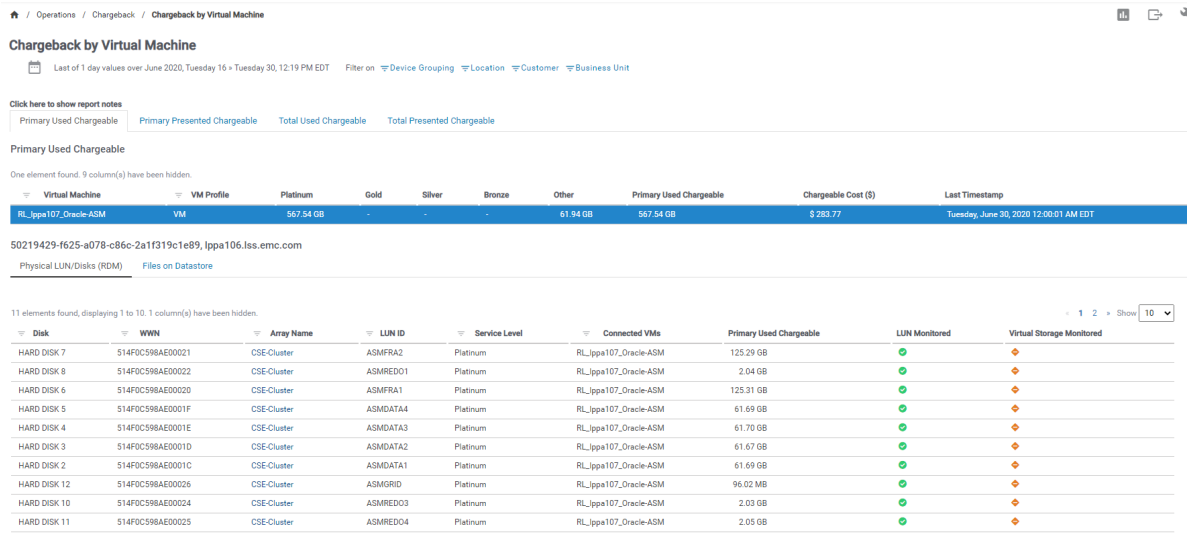

Figure 28

7 Conclusion

In this paper, we discussed the key concepts regarding SRM multi-tenant capabilities. SRM's flexible data model, RBAC security control, integration with external directory sources provide storage administrators the ability to create a secure self-service portal for their customers.

Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

The following resources can be found on Dell Support:

- SRM 4.4 Administration Guide
- SRM 4.4 User Guide for Storage Administrators
- Storage Monitoring and Reporting 4.4 Security Configuration Guide