Veeam ONE

Version 10a

Multi-Tenant Monitoring and Reporting

July, 2020

> **NOTE:**
>
> Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and offices location, visit www.veeam.com/contacts.html.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com

About This Document

This guide provides information about multi-tenant monitoring and reporting functionality in Veeam ONE. The document includes configuration details and a simple example that will guide you through the configuration procedure.

Intended Audience

The guide is designed for anyone who plans to use the Veeam ONE solution. It is primarily aimed at administrators managing virtual environments, but can also be helpful for other current and perspective Veeam ONE users.

About Multi-Tenant Monitoring and Reporting

Veeam ONE supports multi-user access to its monitoring and reporting capabilities. Authorized users can concurrently access the same instance of Veeam ONE to monitor the health state of the virtual infrastructure, view dashboards and run reports.

To restrict access to sensitive infrastructure data, you can limit the scope of virtual infrastructure objects and associated data that must be available to a Veeam ONE user. Thus you can control what subset of the managed virtual infrastructure the user can see and work with.

User permissions can be restricted for two types of inventories:

- VMware vSphere inventory
- vCloud Director inventory

In a multi-tenant environment, you can configure restricted access to Veeam ONE data for owners of virtualized systems or responsible personnel and delegate monitoring and reporting tasks.

For example, if you manage VMware vSphere systems that belong to different business units, you can restrict permissions so that users can monitor and report on systems owned by their business unit. Or, if you manage resources for multiple organizations in a vCloud Director environment, you can restrict permissions on a per-organization basis, so that users can monitor and report on vApps and VMs that belong to their organization.

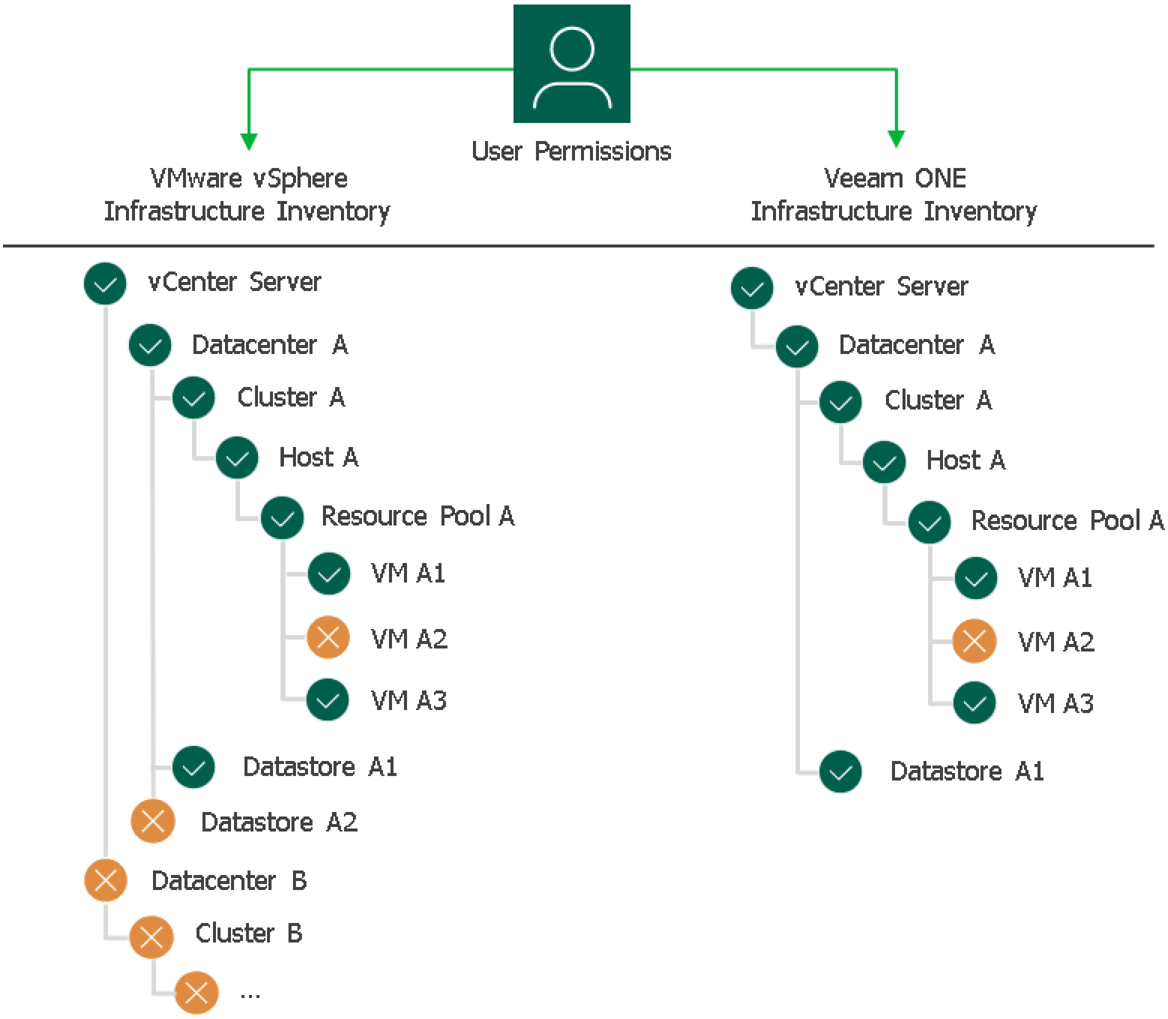
This document describes how to configure permissions for multi-tenant monitoring and reporting in Veeam ONE, and provides a basic configuration example.

How Access to Virtual Infrastructure Objects is Restricted

Veeam ONE collects inventory details about virtual infrastructure objects from connected VMware vSphere and vCloud Director servers. In addition to objects and object properties, Veeam ONE gathers information about user permissions assigned to objects in VMware vSphere and vCloud Director inventories. Permission details are gathered in real time, as part of the regular data collection procedure.

Collected permissions determine what users must (and must not) have access to objects in the Veeam ONE virtual infrastructure inventory. When a user authenticates to Veeam ONE, Veeam ONE checks what permissions are assigned to objects in the VMware vSphere and vCloud Director inventories.

- If the user has appropriate permissions on an object, the user can access this object and associated data in the Veeam ONE infrastructure inventory.
- If the user does not have permissions on an object, the object is hidden. Data associated with this object is unavailable to the user.



Permissions and Security Groups

Do not mix permissions on virtual infrastructure inventory objects with the Veeam ONE security model that is based on security groups.

Users in Security Groups

Security groups define what actions users can perform in Veeam ONE. That is, what part of Veeam ONE functionality is available to users.

- *Veeam ONE Administrators* have access to all functions in Veeam ONE. They can perform all types of actions that Veeam ONE supports, including configuration actions.
- *Veeam ONE Read-Only Users* have limited access to Veeam ONE functions: they can access data in the read-only mode but cannot perform configuration tasks.

Users included in either Veeam ONE security group (*Administrators* or *Read-Only Users*) have access to:

- All Veeam ONE consoles (Veeam ONE Monitor, Veeam ONE Reporter)
- All objects of the infrastructure inventory (including VMware vSphere, vCloud Director, Microsoft Hyper-V and Veeam Backup & Replication)

Users with Restricted Permissions on Virtual Infrastructure Inventory

Permissions define what part of the virtual infrastructure is visible to a Veeam ONE user. To monitor and report on a restricted subset of the virtual infrastructure in Veeam ONE, a user must have permissions assigned on objects of the VMware vSphere or vCloud Director inventory hierarchy. In this case, the user can utilize Veeam ONE monitoring and reporting capabilities for available objects of the VMware vSphere or vCloud Director infrastructure. Microsoft Hyper-V and Veeam Backup & Replication inventory objects will be unavailable for the user.

Note that for users of this type some Veeam ONE functionality is disabled. For details on limitations, see section Functional Restrictions.

> **IMPORTANT!**
>
> Do not include a user with restricted permissions into Veeam ONE security groups. Members of security groups always have access to the whole infrastructure inventory in Veeam ONE, regardless of their permissions on the VMware vSphere or vCloud Director inventory hierarchy.

Functional Restrictions

Users with restricted permissions on the virtual infrastructure inventory have limited access to Veeam ONE functionality. Functional restrictions prevent these users from changing settings that may affect other users in Veeam ONE.

Monitoring

In Veeam ONE Monitor, users with restricted permissions cannot perform the following tasks:

- Access and modify configuration settings (connections to virtual servers, notification settings, Veeam ONE server settings and license).
- Create, modify, delete, acknowledge or resolve alarms.

Reporting

In Veeam ONE Reporter, users with restricted permissions cannot perform the following tasks:

- Access and modify all configuration settings.
- Modify and delete predefined and custom dashboards.
- View custom reports that were saved by other users with restricted permissions.
- Work with specific reports.

  For the list of reports available to these users, see Reports for Users with Restricted Permissions.

Users with restricted permissions can access custom dashboards and saved reports that have been published by *Veeam ONE Administrator*. The virtual infrastructure scope on dashboards and in reports will be restricted in accordance with effective user permissions.

For details on publishing dashboards and reports, see sections Publishing Dashboards and Publishing Reports of the Veeam ONE Reporter Guide.

Configuring Access for Users with Restricted Permissions

To provide access to Veeam ONE reporting and monitoring features for a user with restricted permissions, perform these steps:

1. Check Veeam ONE security group membership.
2. Check requirements to the user account.
3. Assign permissions on the VMware vSphere or vCloud Director inventory objects.
4. Log in to Veeam ONE as the user.

Step 1. Check Veeam ONE Security Group Membership

Check that the user is **not included** in Veeam ONE security groups (*Veeam ONE Administrators* or *Veeam ONE Read-Only Users*). Otherwise, the user will be granted access to the whole infrastructure inventory in Veeam ONE, including VMware vSphere, vCloud Director, Microsoft Hyper-V and Veeam Backup & Replication.

For details, see Permissions and Security Groups.

Step 2. Check Requirements to the User Account

You can provide access to Veeam ONE for single users and user groups.

The following table describes types of accounts for which you can configure restricted permissions.

Platform	Account Type	Description and Notes
vCenter Server	Domain users and groups	Members of the Active Directory domain. vCenter Server must be configured to use Active Directory for authentication. For details on user authentication in VMware vSphere, see Active Directory Identity Source Settings. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.
	Local users and groups	Local users and groups on the machine where vCenter Server is installed. To log in to Veeam ONE, you must provide user name in the following format: `hostname\username`.
	Single Sign-On users and groups	Single Sign-On users and groups on vCenter Server. For details, see vSphere Authentication with vCenter Single Sign-On. **Note**: Single Sign-On must be installed on the machine where vCenter Server runs, with the default installation path and port settings. Otherwise, Veeam ONE will not be able to detect its database with user groups and users. To log in to Veeam ONE, you must provide user name in the following format: `ssodomain\username`.
ESXi host	Domain users and groups	Members of the Active Directory domain. Standalone hosts must be configured to use Active Directory for authentication. For details, see Using Active Directory to Manage ESXi Users. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.

Platform	Account Type	Description and Notes
vCloud Director	Domain users and groups	Members of the Active Directory domain. Users must be able to authenticate against an LDAP server. For details, see Configuring the System LDAP Settings. To log in to Veeam ONE, you must provide user name in the following format: `domain\username`.
	Local users and groups	Local users and groups in vCloud Director. To log in to Veeam ONE, you must provide user name in the following format: • For organization user: `organization\username` • For vCloud Director administrator: `system\username`

> **NOTE:**
>
> For each local or Single Sign-On user that authenticates to Veeam ONE, Veeam ONE creates a temporary Windows account on the machine that runs the Veeam ONE Server component. This temporary account is deleted after 30 days of inactivity.

Authorizing with Veeam ONE

To authorize with Veeam ONE components (Veeam ONE Monitor and Veeam ONE Reporter), a user must have the *Allow log on locally* privilege assigned.

By default, this privilege is assigned to users included in the local Administrators group. For users not included in the local Administrators group, you must assign this privilege manually.

> **NOTE:**
>
> If you use the advanced deployment scenario, you must assign the *Allow log on locally* privilege on the machines that host the Veeam ONE Server and Veeam ONE Web UI components.

Step 3. Assign Permissions on Infrastructure Inventory Objects

To view and work with virtual infrastructure objects in Veeam ONE, the user must have appropriate permissions on these objects set in the VMware vSphere or vCloud Director inventory.

VMware vSphere Permissions

Connect to vCenter Server or standalone host with vSphere Client and assign permissions on objects to which the user must have access.

The following table shows minimal required privileges on VMware vSphere inventory objects.

vCenter Server (root) **Data Center** **Cluster** **Host** **Resource Pool/vApp** **Datastore Cluster** **Datastore**	Read-only
Virtual Machine	• Read-only • Virtual machine.Interaction.Answer question[1] • Virtual machine.Interaction.Console interaction[1]

[1] Required to access VM console in Veeam ONE Monitor

> NOTE:
>
> If you assign permissions to container objects (such as hosts, resource pools or vApps), consider enabling propagation. In this case, all new child objects that might added to the container in future will become available to the user.

vCloud Director Permissions

Connect to vCloud Director and assign permissions on objects to which the user must have access.

The following table shows minimal required roles for vCloud Director inventory objects.

VI Inventory Object	vCloud Director Role
vCloud Director (root)	System Administrator
Organization	Console access only

Step 4. Log in to Veeam ONE as the User

Log in to Veeam ONE Monitor and Veeam ONE Reporter as the user to make sure the user has access to Veeam ONE.

How to Log in to Veeam ONE Monitor

To log in to Veeam ONE Monitor:

1. Launch Veeam ONE Monitor Client.

   Veeam ONE Monitor Client can be installed together with the Veeam ONE Server component, or on another machine — for example, on the user's workstation. For details on installing a standalone instance of Veeam ONE Monitor Client, see section Installing Veeam ONE Monitor Client of the Veeam ONE Deployment Guide.

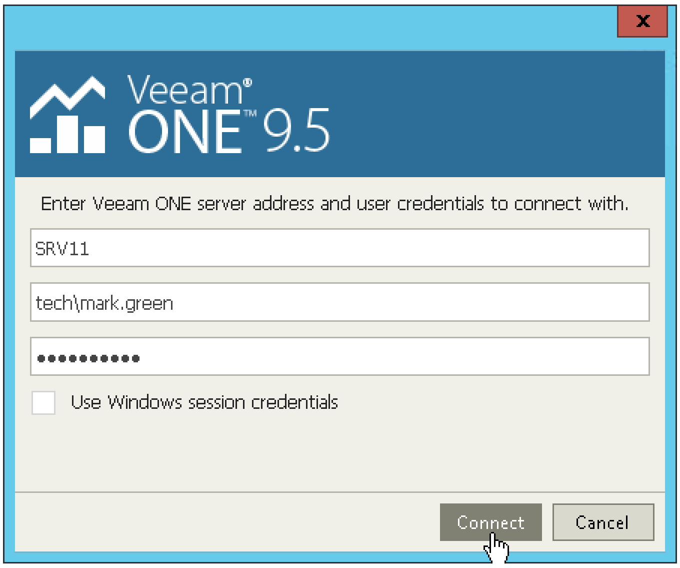
2. In the authentication window, specify the name of the server where the Veeam ONE Server component runs.

   The format of the user name depends on the user account type. For details on supported login formats, see table in Step 2. Check Requirements to the User Account.

   You can select the **Use Windows session credentials** check box. In this case, you will connect to Veeam ONE Monitor using credentials of the account under which you are logged on. Authentication under Windows session credentials is possible only for domain users working with VMware vSphere and vCloud Director environments. Non-domain users must type user credentials explicitly in the authentication window.

> NOTE:
>
> To be able to authenticate using Windows session credentials, you must log in to Veeam ONE Monitor at least once with user credentials specified explicitly. After this, you can use the **Use Windows session credentials** check box for authentication.

3. Click **Connect**.



Enter Veeam ONE server address and user credentials to connect with.

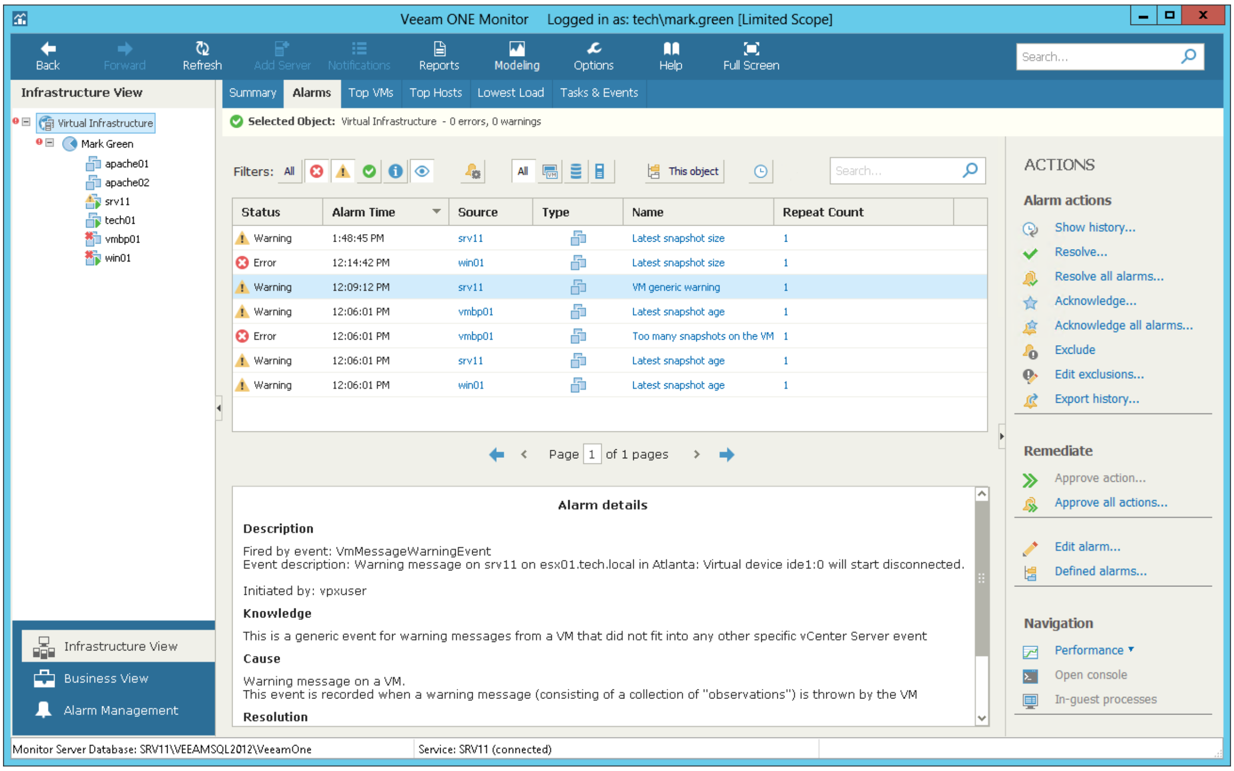
SRV11

tech\mark.green

●●●●●●●●●●

□ Use Windows session credentials

4. After you log in, check the top of the console. Veeam ONE Monitor will display the *[Limited scope]* label next to the user name under which you are logged in.



Selected Object: Virtual Infrastructure - 0 errors, 0 warnings

Status	Alarm Time	Source	Type	Name	Repeat Count
Warning	1:48:45 PM	srv11		Latest snapshot size	1
Error	12:14:42 PM	win01		Latest snapshot size	1
Warning	12:09:12 PM	srv11		VM generic warning	1
Warning	12:06:01 PM	vmbp01		Latest snapshot age	1
Error	12:06:01 PM	vmbp01		Too many snapshots on the VM	1
Warning	12:06:01 PM	srv11		Latest snapshot age	1
Warning	12:06:01 PM	win01		Latest snapshot age	1

Page 1 of 1 pages

Alarm details

Description

Fired by event: VmMessageWarningEvent
Event description: Warning message on srv11 on esx01.tech.local in Atlanta: Virtual device ide1:0 will start disconnected.

Initiated by: vpxuser

Knowledge

This is a generic event for warning messages from a VM that did not fit into any other specific vCenter Server event

Cause

Warning message on a VM.
This event is recorded when a warning message (consisting of a collection of "observations") is thrown by the VM

Resolution

Monitor Server Database: SRV11\VEEAMSQL2012\VeeamOne

Service: SRV11 (connected)

How to Log in to Veeam ONE Reporter

To log in to Veeam ONE Reporter:

1. Access the Veeam ONE Reporter website.

   For details on accessing Veeam ONE Reporter, see section Accessing Veeam ONE Monitor and Reporter of the Veeam ONE Deployment Guide.

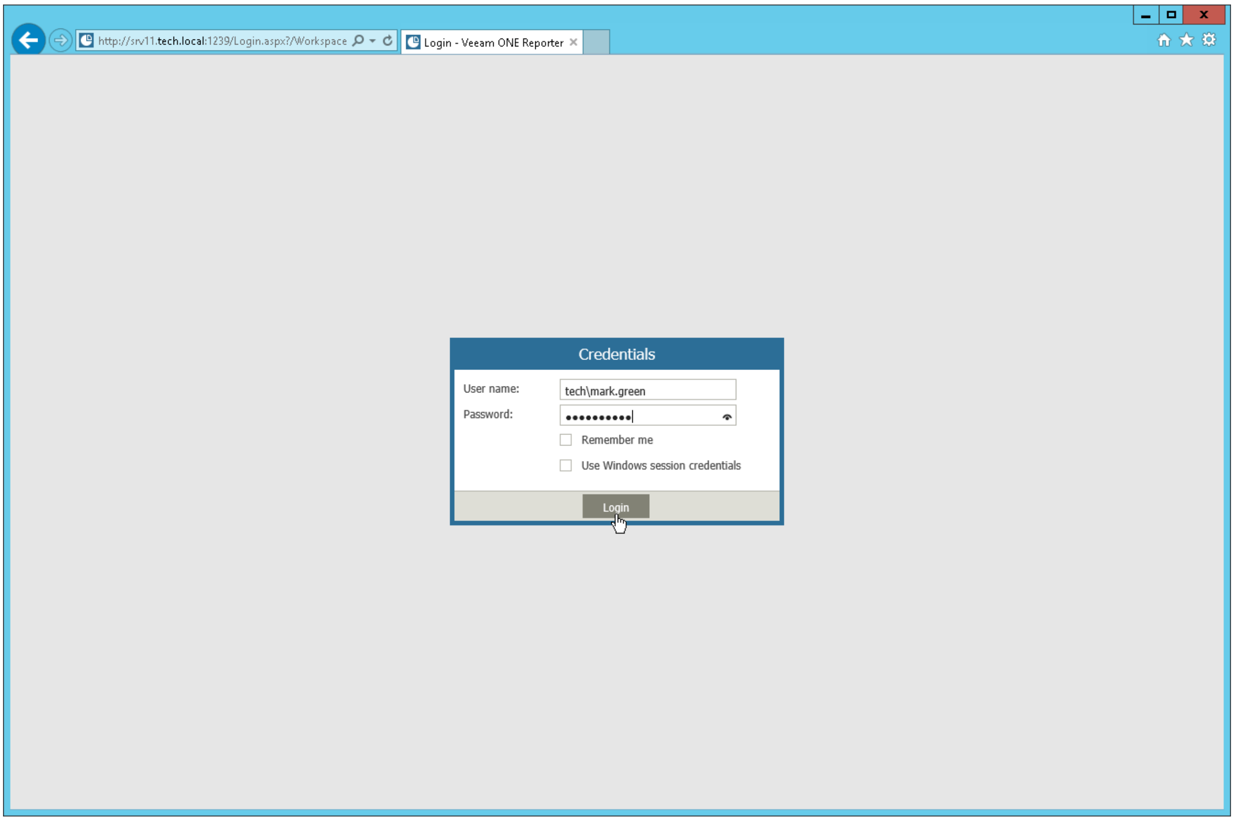
2. In the **Credentials** window, specify a user name and password of a user account.

   The format of the user name depends on the user account type. For details on supported login formats, see table in Step 2. Check Requirements to the User Account.

   [For Internet Explorer] You can select the **Use Windows session credentials** check box. In this case, you will connect to Veeam ONE Reporter using credentials of the account under which you are logged on. Authentication under Windows session credentials is possible only for domain users working with VMware vSphere and vCloud Director environments. Non-domain users must type user credentials explicitly in the authentication window.

> **NOTE:**
>
> To be able to authenticate using Windows session credentials, you must log in to Veeam ONE Reporter at least once with user credentials specified explicitly. After this, you can use the **Use Windows session credentials** check box for authentication.

3. Click **Login**.



http://srv11.tech.local:1239/Login.aspx?/Workspace

Login - Veeam ONE Reporter

Credentials

User name: tech\mark.green

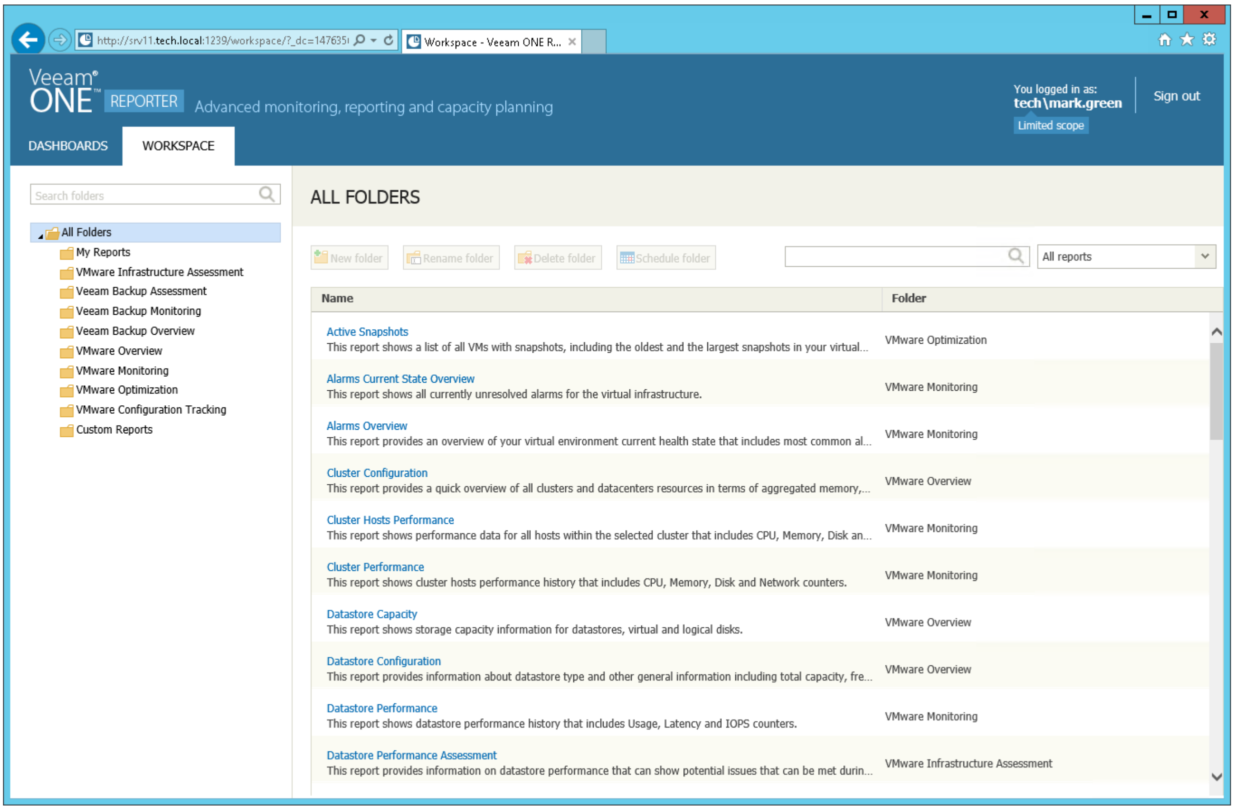
Password: ••••••••••

□ Remember me

□ Use Windows session credentials

Login

4. After you log in, check the top right corner. Veeam ONE Reporter will display the *Limited scope* label next to the user name under which you are logged in.



http://srv11.tech.local:1239/workspace/?_dc=147635

Workspace - Veeam ONE R...

Veeam® ONE™ REPORTER Advanced monitoring, reporting and capacity planning

You logged in as: tech\mark.green Limited scope

Sign out

ALL FOLDERS

Name	Folder
Active Snapshots This report shows a list of all VMs with snapshots, including the oldest and the largest snapshots in your virtual...	VMware Optimization
Alarms Current State Overview This report shows all currently unresolved alarms for the virtual infrastructure.	VMware Monitoring
Alarms Overview This report provides an overview of your virtual environment current health state that includes most common al...	VMware Monitoring
Cluster Configuration This report provides a quick overview of all clusters and datacenters resources in terms of aggregated memory,...	VMware Overview
Cluster Hosts Performance This report shows performance data for all hosts within the selected cluster that includes CPU, Memory, Disk an...	VMware Monitoring
Cluster Performance This report shows cluster hosts performance history that includes CPU, Memory, Disk and Network counters.	VMware Monitoring
Datastore Capacity This report shows storage capacity information for datastores, virtual and logical disks.	VMware Overview
Datastore Configuration This report provides information about datastore type and other general information including total capacity, fre...	VMware Overview
Datastore Performance This report shows datastore performance history that includes Usage, Latency and IOPS counters.	VMware Monitoring
Datastore Performance Assessment This report provides information on datastore performance that can show potential issues that can be met durin...	VMware Infrastructure Assessment

Configuration Example

This section provides an example on how to configure permissions for Veeam ONE virtual infrastructure inventory. The example is based on the following scenario:

> Virtualized systems in your virtual environment are grouped into resource pools. Each resource pool belongs to one user — the owner of VMs.
>
> To protect VMs within the virtual environment, you use Veeam Backup & Replication. To monitor and report on the data protection status, you deployed Veeam ONE and integrated it with Veeam Backup & Replication.
>
> A resource pool owner, *Mark Green*, wants to track the data protection status for his VMs. You need to provide access to Veeam ONE for this user and restrict permissions to his resource pool and all contents within it.

This example assumes that you completed these prerequisites:

1. Deployed Veeam Backup & Replication, configured backup or replication jobs for user's VMs and ran these jobs at least once.
2. Deployed Veeam ONE, connected a vCenter Server and a Veeam backup server to it.

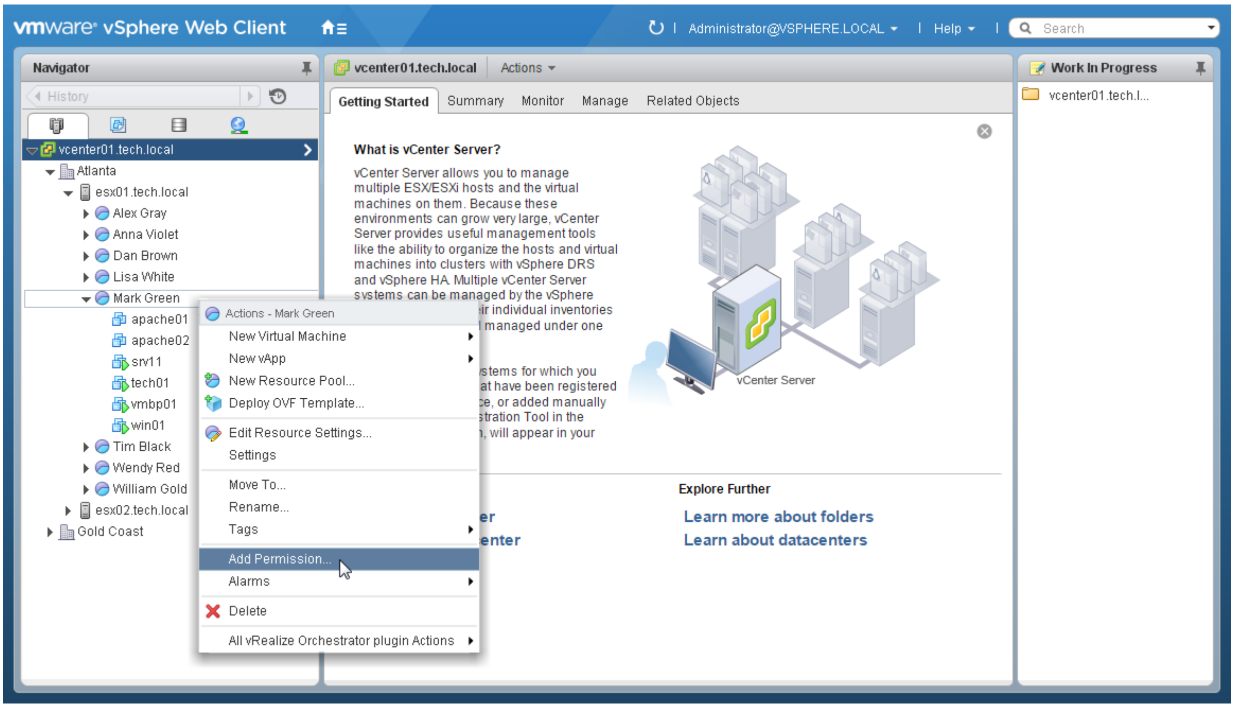
To restrict permissions to user's resource pool in Veeam ONE, perform these steps:

1. Configure permissions in vCenter Server.
2. Create the Protected VMs report as the user.
3. Create the Protected VMs report as the administrator.

Step 1. Configure Permissions in vCenter Server

Log in to the VMware vSphere Client as administrator and assign permissions on the resource pool to the owner user:

1. In the infrastructure hierarchy, right-click a resource pool node that belongs to Mark Green and choose **Add Permission**.



What is vCenter Server?

vCenter Server allows you to manage multiple ESX/ESXi hosts and the virtual machines on them. Because these environments can grow very large, vCenter Server provides useful management tools like the ability to organize the hosts and virtual machines into clusters with vSphere DRS and vSphere HA. Multiple vCenter Server systems can be managed by the vSphere ...ir individual inventories ...managed under one

...stems for which you ...at have been registered ...ce, or added manually ...stration Tool in the ...), will appear in your

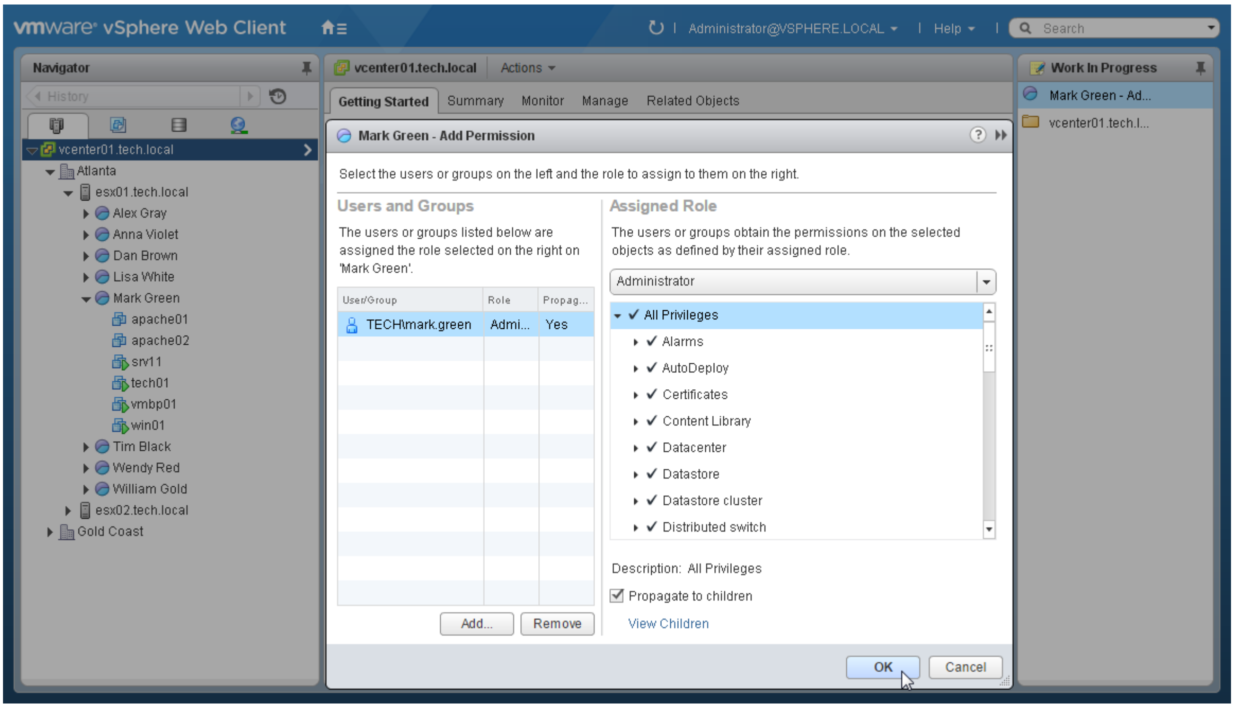
2. In the **Add Permissions** window, add the resource pool owner to the **Users and Groups** list.

3. In the **Assigned Role** list, choose the **Administrator** role.

   Instead of giving administrator privileges, you can create a custom role with minimal privileges required by Veeam ONE. For details on required privileges, see VMware vSphere Permissions.

4. Select the **Propagate to children** check box.

5. Click **OK**.



Mark Green - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'Mark Green'.

User/Group	Role	Propag...
TECH\mark.green	Admi...	Yes

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

- ✓ All Privileges
  - ✓ Alarms
  - ✓ AutoDeploy
  - ✓ Certificates
  - ✓ Content Library
  - ✓ Datacenter
  - ✓ Datastore
  - ✓ Datastore cluster
  - ✓ Distributed switch

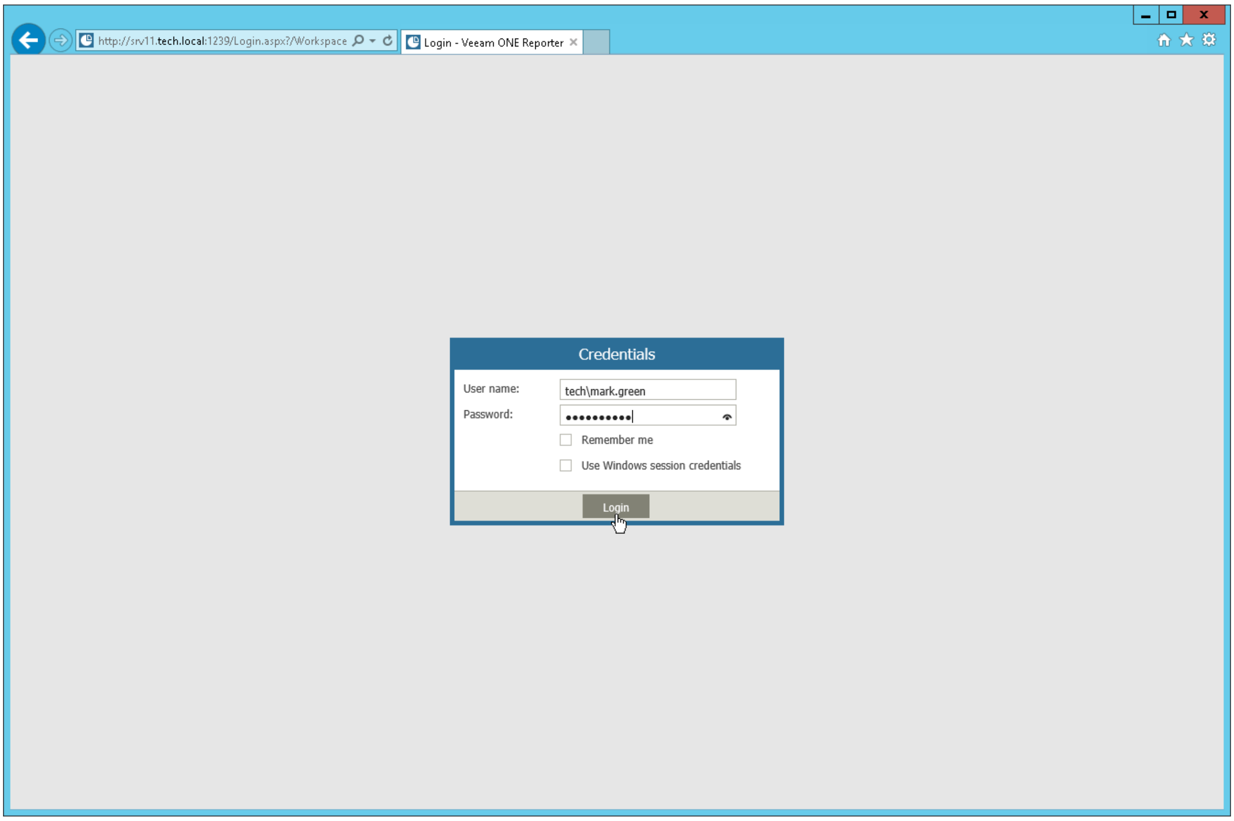
Description: All Privileges

☑ Propagate to children

Step 2. Create the Protected VMs Report as the User

Create the Protected VMs report as Mark Green to check that its scope is limited to VMs within Mark's resource pool.

1. Navigate to the Veeam ONE Reporter website.
2. In the **Credentials** window, specify user name and password of Mark Green.
3. Click **Login**.



http://srv11.tech.local:1239/Login.aspx?/Workspace
Login - Veeam ONE Reporter
Credentials
Login

User name: tech\mark.green

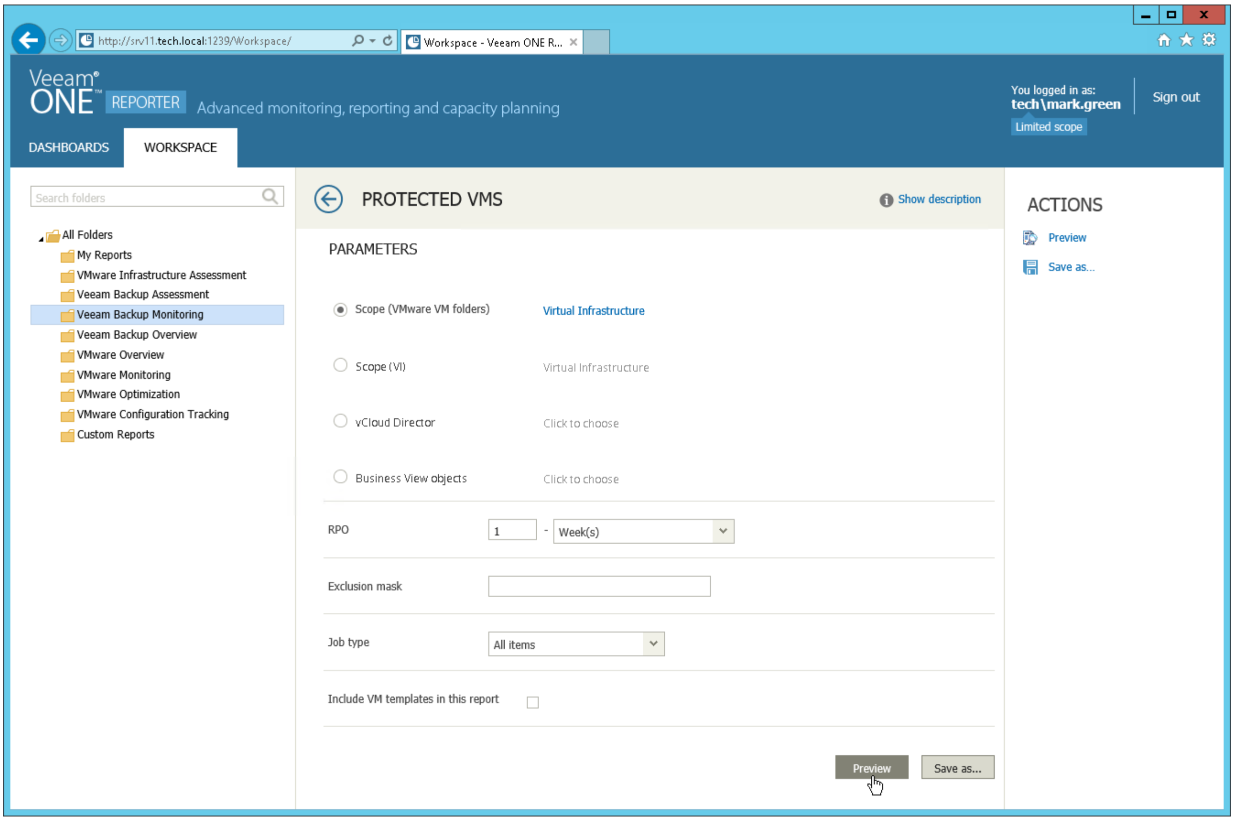
Password: ●●●●●●●●●●

□ Remember me

□ Use Windows session credentials

4. In Veeam ONE Reporter, open the **Workspace** tab.
5. In the list of report packs on the left, select **Veeam Backup Monitoring**.
6. In the list of reports on the right, select **Protected VMs**.

7. Change the report parameters if required and in the **Actions** pane on the right click **Create Report**.



PROTECTED VMS

PARAMETERS

● Scope (VMware VM folders) — Virtual Infrastructure

○ Scope (VI) — Virtual Infrastructure

○ vCloud Director — Click to choose

○ Business View objects — Click to choose

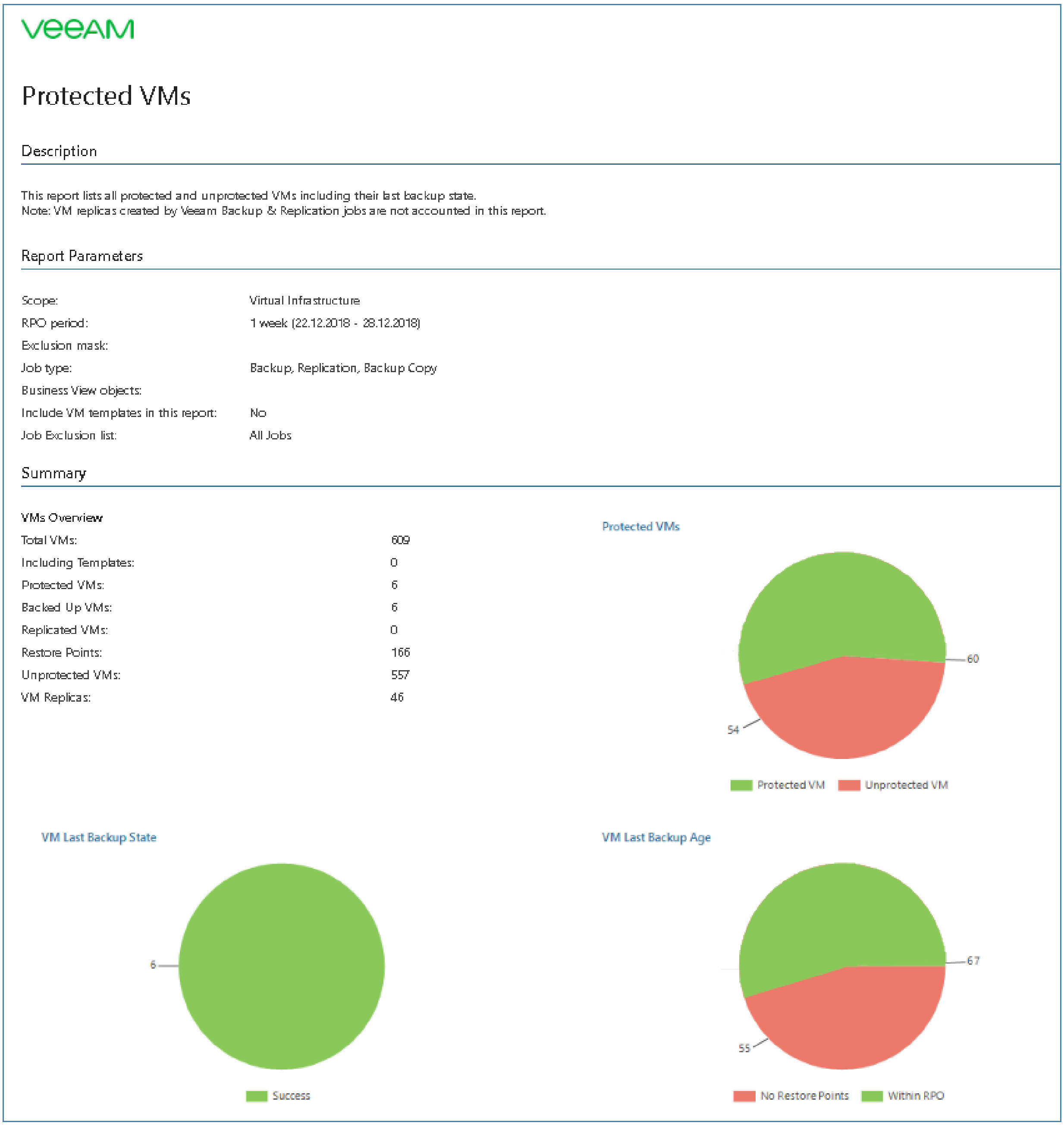
RPO: 1 - Week(s)

Exclusion mask:

Job type: All items

Include VM templates in this report □

8. Check that the report scope is limited to VMs within the resource pool owned by Mark Green.



Protected VMs

Description

This report lists all protected and unprotected VMs including their last backup state.
Note: VM replicas created by Veeam Backup & Replication jobs are not accounted in this report.

Report Parameters

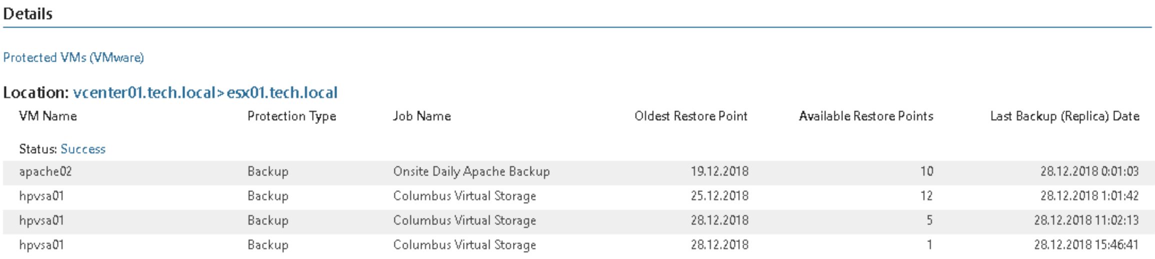
Scope:	Virtual Infrastructure
RPO period:	1 week (22.12.2018 - 28.12.2018)
Exclusion mask:	
Job type:	Backup, Replication, Backup Copy
Business View objects:	
Include VM templates in this report:	No
Job Exclusion list:	All Jobs

Summary

VMs Overview

Total VMs:	609
Including Templates:	0
Protected VMs:	6
Backed Up VMs:	6
Replicated VMs:	0
Restore Points:	166
Unprotected VMs:	557
VM Replicas:	46

9. Switch to the second report page and check the backup state for VMs in the resource pool.



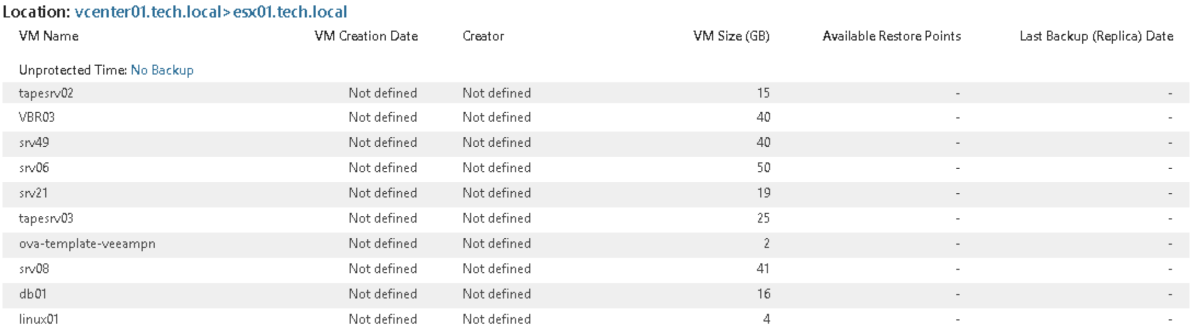
Details

Protected VMs (VMware)

Location: vcenter01.tech.local>esx01.tech.local

VM Name	Protection Type	Job Name	Oldest Restore Point	Available Restore Points	Last Backup (Replica) Date
Status: Success					
apache02	Backup	Onsite Daily Apache Backup	19.12.2018	10	28.12.2018 0:01:03
hpvsa01	Backup	Columbus Virtual Storage	25.12.2018	12	28.12.2018 1:01:42
hpvsa01	Backup	Columbus Virtual Storage	28.12.2018	5	28.12.2018 11:02:13
hpvsa01	Backup	Columbus Virtual Storage	28.12.2018	1	28.12.2018 15:46:41

10. Switch to the third report page and check the list of unprotected VMs in the resource pool.



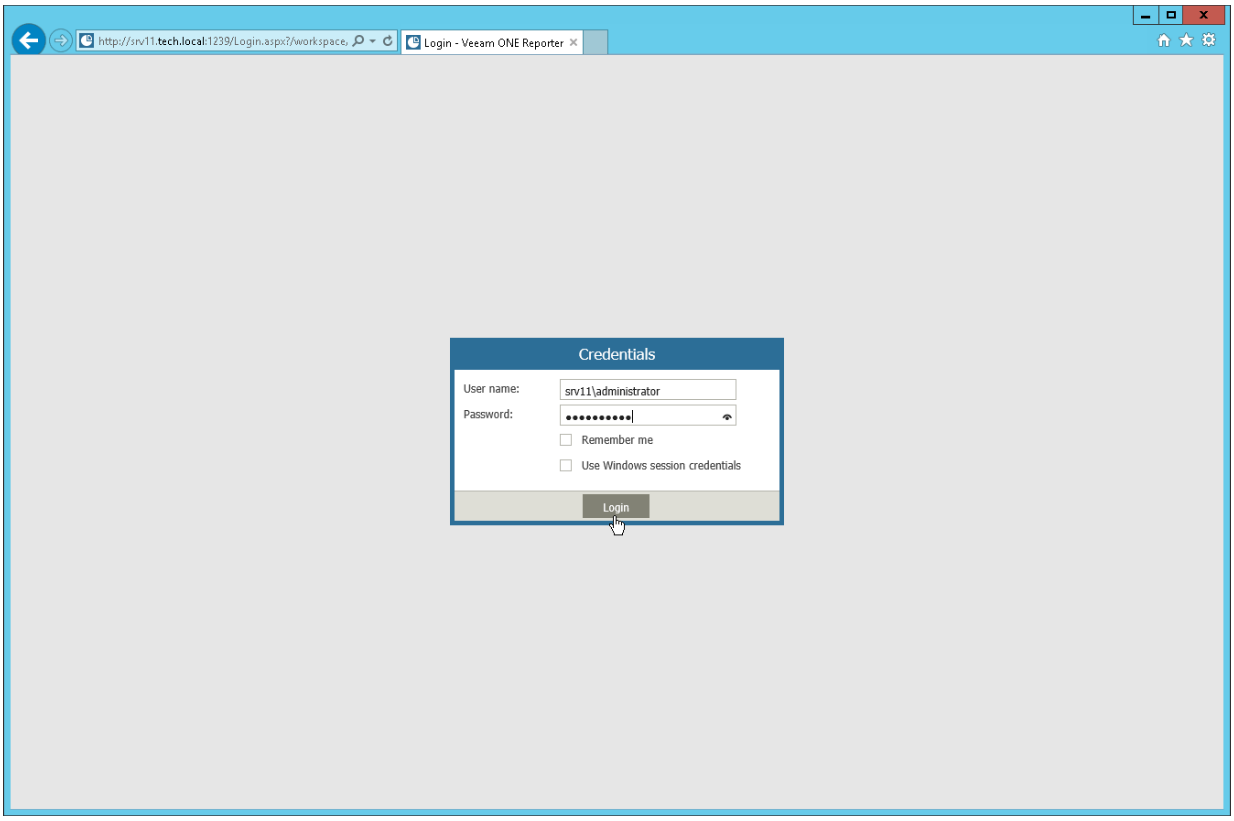
Location: vcenter01.tech.local>esx01.tech.local

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
tapesrv02	Not defined	Not defined	15	-	-
VBR03	Not defined	Not defined	40	-	-
srv49	Not defined	Not defined	40	-	-
srv06	Not defined	Not defined	50	-	-
srv21	Not defined	Not defined	19	-	-
tapesrv03	Not defined	Not defined	25	-	-
ova-template-veeampn	Not defined	Not defined	2	-	-
srv08	Not defined	Not defined	41	-	-
db01	Not defined	Not defined	16	-	-
linux01	Not defined	Not defined	4	-	-

Step 3. Create the Protected VMs Report as the Administrator

Create the Protected VMs report as Veeam ONE Administrator and check the scope that the report will return. Compare the report output for the user and administrator.

1. Navigate to the Veeam ONE Reporter website.
2. In the **Credentials** window, specify a user name and password of the administrator.
3. Click **Login**.



http://srv11.tech.local:1239/Login.aspx?/workspace,

Login - Veeam ONE Reporter

Credentials

User name: srv11\administrator

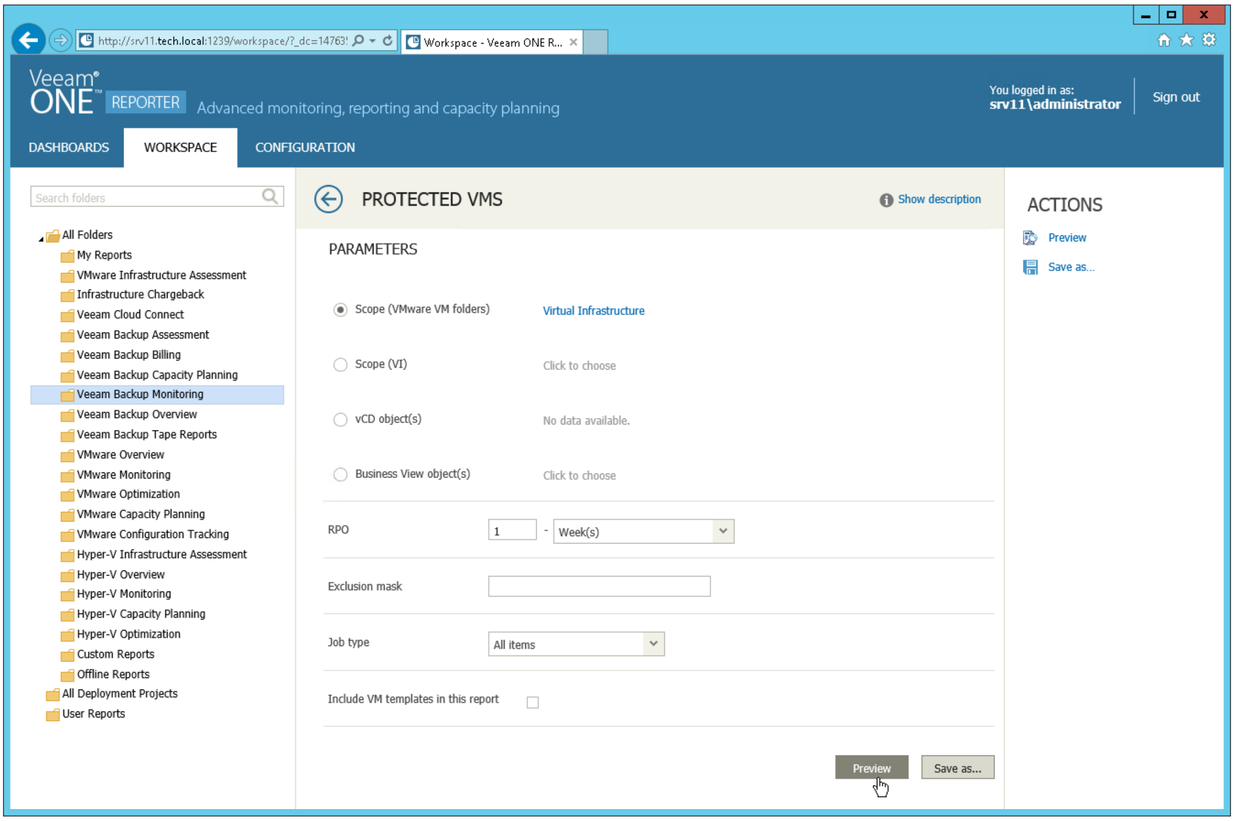
Password: ●●●●●●●●●●●

□ Remember me

□ Use Windows session credentials

4. In Veeam ONE Reporter, open the **Workspace** tab.
5. In the list of report packs on the left, select **Veeam Backup Monitoring**.
6. In the list of reports on the right, select **Protected VMs**.

7. Change the report parameters if required and in the **Actions** pane on the right click **Create Report**.



PROTECTED VMS

PARAMETERS

● Scope (VMware VM folders) — Virtual Infrastructure

○ Scope (VI) — Click to choose

○ vCD object(s) — No data available.

○ Business View object(s) — Click to choose

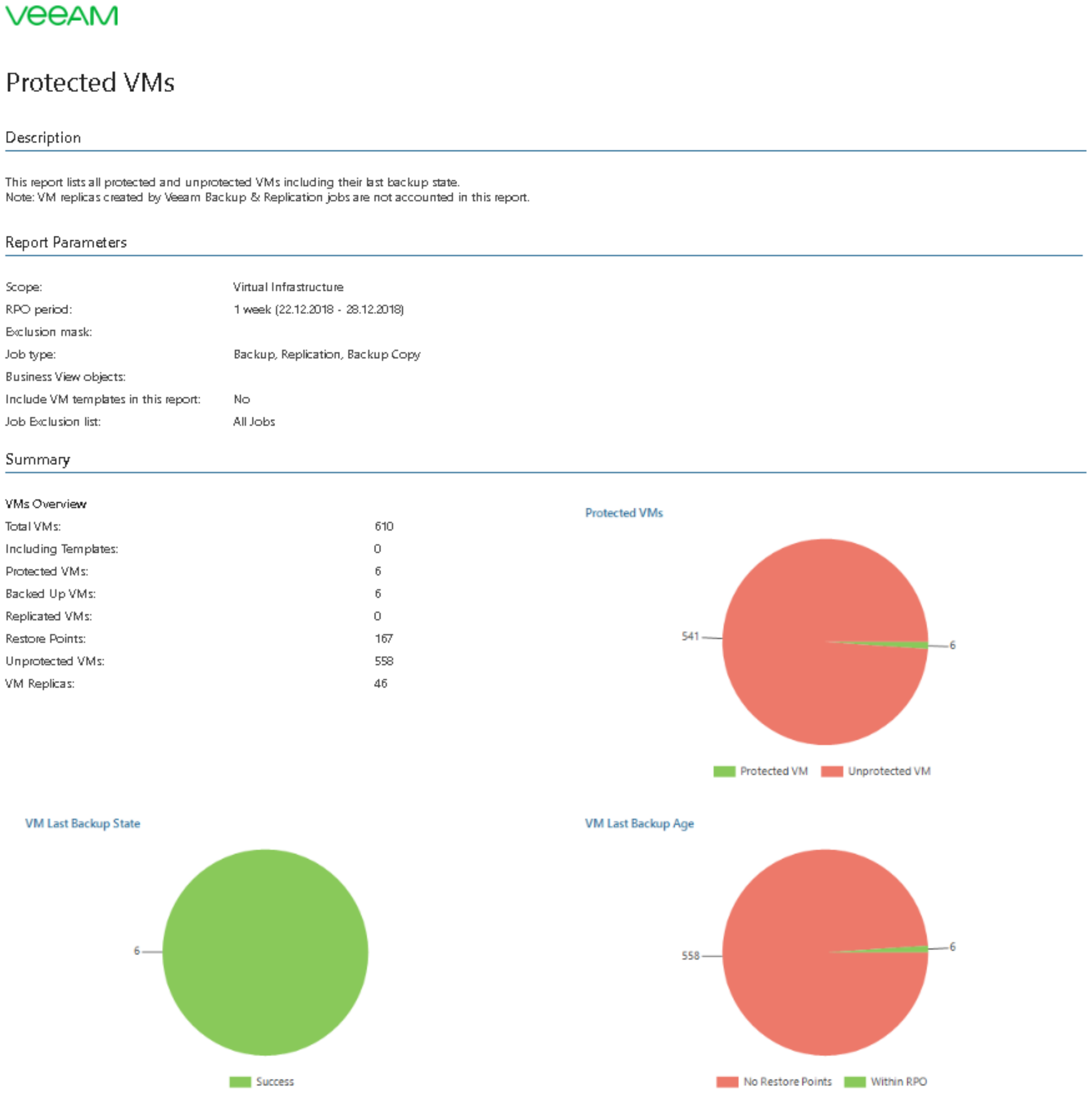
RPO: 1 - Week(s)

Exclusion mask:

Job type: All items

Include VM templates in this report □

8. Check that the report scope includes all VMs within the managed virtual environment.



VEEAM

Protected VMs

Description

This report lists all protected and unprotected VMs including their last backup state.
Note: VM replicas created by Veeam Backup & Replication jobs are not accounted in this report.

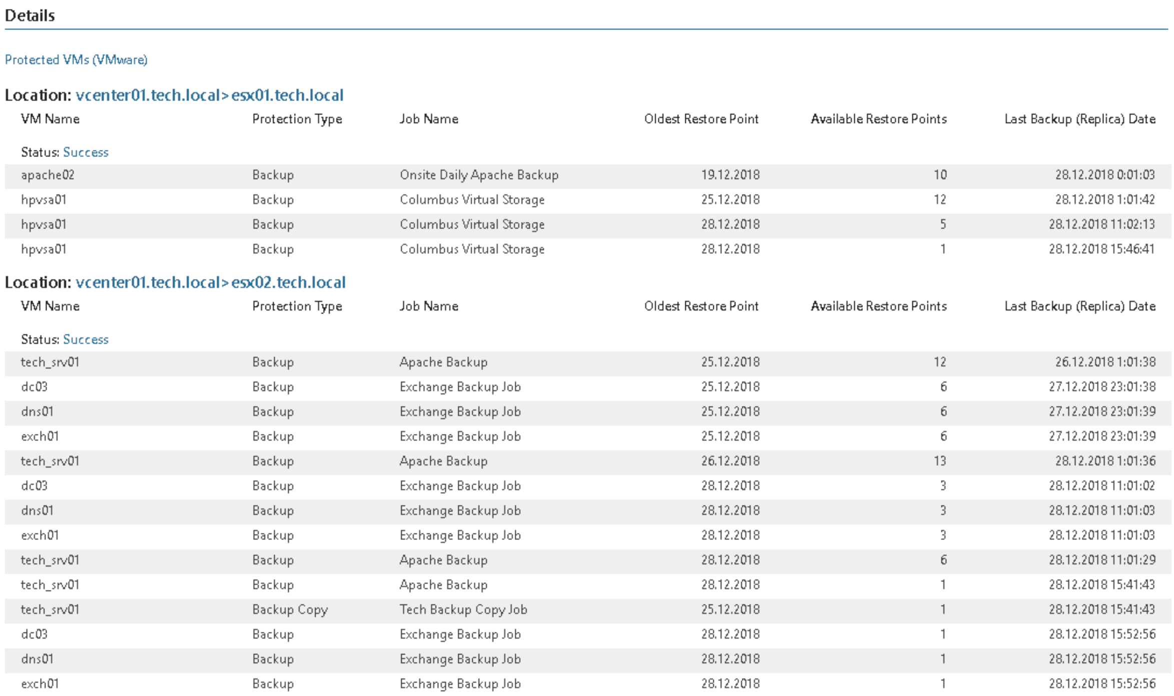
Report Parameters

Scope:	Virtual Infrastructure
RPO period:	1 week (22.12.2018 - 28.12.2018)
Exclusion mask:	
Job type:	Backup, Replication, Backup Copy
Business View objects:	
Include VM templates in this report:	No
Job Exclusion list:	All Jobs

Summary

VMs Overview	
Total VMs:	610
Including Templates:	0
Protected VMs:	6
Backed Up VMs:	6
Replicated VMs:	0
Restore Points:	167
Unprotected VMs:	558
VM Replicas:	46

9. Switch to the second report page to check the list of protected VMs in the managed environment.



Details

Protected VMs (VMware)

Location: vcenter01.tech.local > esx01.tech.local

Status: Success

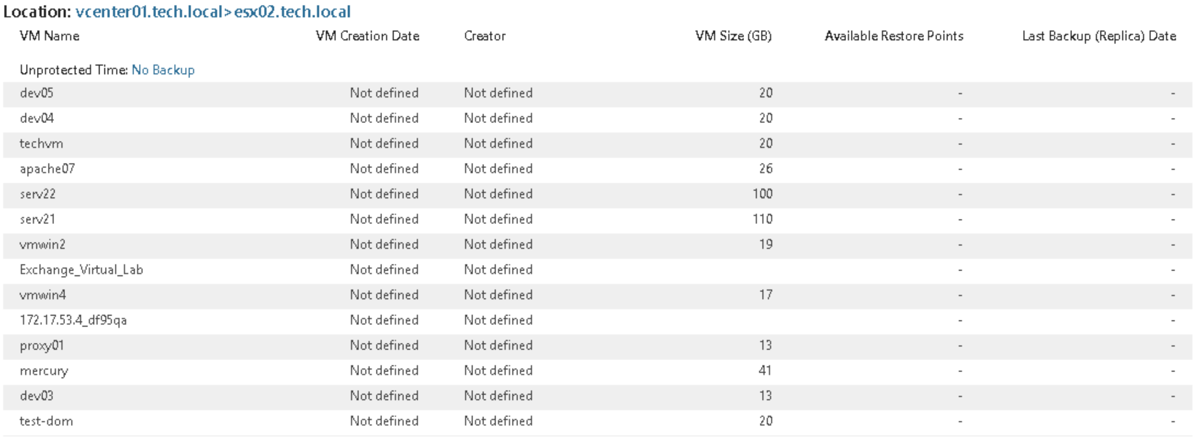
VM Name	Protection Type	Job Name	Oldest Restore Point	Available Restore Points	Last Backup (Replica) Date
apache02	Backup	Onsite Daily Apache Backup	19.12.2018	10	28.12.2018 0:01:03
hpvsa01	Backup	Columbus Virtual Storage	25.12.2018	12	28.12.2018 1:01:42
hpvsa01	Backup	Columbus Virtual Storage	28.12.2018	5	28.12.2018 11:02:13
hpvsa01	Backup	Columbus Virtual Storage	28.12.2018	1	28.12.2018 15:46:41

Location: vcenter01.tech.local > esx02.tech.local

Status: Success

VM Name	Protection Type	Job Name	Oldest Restore Point	Available Restore Points	Last Backup (Replica) Date
tech_srv01	Backup	Apache Backup	25.12.2018	12	26.12.2018 1:01:38
dc03	Backup	Exchange Backup Job	25.12.2018	6	27.12.2018 23:01:38
dns01	Backup	Exchange Backup Job	25.12.2018	6	27.12.2018 23:01:39
exch01	Backup	Exchange Backup Job	25.12.2018	6	27.12.2018 23:01:39
tech_srv01	Backup	Apache Backup	26.12.2018	13	28.12.2018 1:01:36
dc03	Backup	Exchange Backup Job	28.12.2018	3	28.12.2018 11:01:02
dns01	Backup	Exchange Backup Job	28.12.2018	3	28.12.2018 11:01:03
exch01	Backup	Exchange Backup Job	28.12.2018	3	28.12.2018 11:01:03
tech_srv01	Backup	Apache Backup	28.12.2018	6	28.12.2018 11:01:29
tech_srv01	Backup	Apache Backup	28.12.2018	1	28.12.2018 15:41:43
tech_srv01	Backup Copy	Tech Backup Copy Job	25.12.2018	1	28.12.2018 15:41:43
dc03	Backup	Exchange Backup Job	28.12.2018	1	28.12.2018 15:52:56
dns01	Backup	Exchange Backup Job	28.12.2018	1	28.12.2018 15:52:56
exch01	Backup	Exchange Backup Job	28.12.2018	1	28.12.2018 15:52:56

10. Switch to the third report page and check the list of unprotected VMs in the managed environment.



Location: vcenter01.tech.local > esx02.tech.local

Unprotected Time: No Backup

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
dev05	Not defined	Not defined	20	-	-
dev04	Not defined	Not defined	20	-	-
techvm	Not defined	Not defined	20	-	-
apache07	Not defined	Not defined	26	-	-
serv22	Not defined	Not defined	100	-	-
serv21	Not defined	Not defined	110	-	-
vmwin2	Not defined	Not defined	19	-	-
Exchange_Virtual_Lab	Not defined	Not defined		-	-
vmwin4	Not defined	Not defined	17	-	-
172.17.53.4_df95qa	Not defined	Not defined		-	-
proxy01	Not defined	Not defined	13	-	-
mercury	Not defined	Not defined	41	-	-
dev03	Not defined	Not defined	13	-	-
test-dom	Not defined	Not defined	20	-	-

Reports for Users with Restricted Permissions

The following reports are available to users with restricted permissions:

Report Pack	Report	Available for VMware vSphere users	Available for vCloud Director users
Infrastructure Chargeback	VM Configuration Chargeback	Yes	Yes
	VM Performance Chargeback	Yes	Yes
VMware Infrastructure Assessment	Datastore Performance Assessment	Yes	No
	VM Change Rate Estimation	Yes	Yes
	VM Configuration Assessment	Yes	Yes
Veeam Backup Assessment	VM Backup Compliance Overview	Yes	Yes
	VMs with no Archive Copy	Yes	Yes
Veeam Backup Monitoring	Protected VMs	Yes	Yes
	VM Daily Protection Status	Yes	No
	VM Change Rate History	Yes	Yes
Veeam Backup Overview	Protected VMs Job Schedule	Yes	Yes
VMware Overview	Cluster Configuration	Yes	No
	Datastore Capacity	Yes	No

Report Pack	Report	Available for VMware vSphere users	Available for vCloud Director users
	Datastore Configuration	Yes	No
	Datastore Space Usage History	Yes	No
	Guest Disk Free Space	Yes	No
	Host Configuration	Yes	No
	Hypervisor Version	Yes	No
	Infrastructure Overview	Yes	No
	VMs Configuration	Yes	No
	VMs Growth	Yes	No
VMware Monitoring	Alarms Current State Overview	Yes	No
	Alarms Overview	Yes	No
	Cluster Hosts Performance	Yes	No
	Cluster Performance	Yes	No
	Datastore Performance	Yes	No
	Host Performance	Yes	No
	Host Uptime	Yes	No
	Multiple Clusters Performance	Yes	No
	Resource Pool and vApp Performance	Yes	No

Report Pack	Report	Available for VMware vSphere users	Available for vCloud Director users
	VM Performance	Yes	Yes
	VM Uptime	Yes	No
VMware Optimization	Active Snapshots	Yes	Yes
	Garbage Files	Yes	No
	Idle VMs	Yes	Yes
	Inefficient Datastore Usage	Yes	Yes
	Orphaned VM Snapshots	Yes	No
	Oversized VMs	Yes	Yes
	Powered Off VMs	Yes	Yes
	Undersized VMs	Yes	Yes
VMware Configuration Tracking	Infrastructure Changes Audit	Yes	No
	Infrastructure Changes by Object	Yes	No
Custom reports	VMware Custom Performance	Yes	Yes
	VMware Raw Performance Data	Yes	No
vCloud Director	Catalogs Overview	Yes	Yes
	Organization Configuration	Yes	Yes

Report Pack	Report	Available for VMware vSphere users	Available for vCloud Director users
	Organization vDC Performance	Yes	Yes
	Provider vDC Performance	Yes	Yes
	vApp Configuration	Yes	Yes
	vApp Performance	Yes	Yes
	VM Uptime	Yes	Yes