



# Recovery as a Service with PlateSpin Protect 11.1

*Best Practices & Reference Architecture*



## Table of Contents

Introduction to PlateSpin Protect. . . . .	3
Why is “Recovery as a Service” a Special Use Case? . . . . .	3
Multi-Tenancy in the VMware Back-End Infrastructure . . . . .	4
Reference Architecture Diagram . . . . .	4
Explanation of the Architectural Components . . . . .	4
Defining the VMware Roles . . . . .	5
Basic Command Line Syntax . . . . .	5
Assigning the New Roles to Objects and Resources in vCenter . . . . .	6
Rebranding PlateSpin Protect 11.1 . . . . .	9
High-Level Overview . . . . .	9
Image-Based Replication Seeding . . . . .	11
High-Level Overview . . . . .	11
Setup Procedure . . . . .	11
MTU Tuning for Replication Traffic . . . . .	12
Multi-tenancy for Microsoft SQL Server 2014 . . . . .	13
About NetIQ. . . . .	15



## Introduction to PlateSpin Protect

This document describes how Service Providers can use PlateSpin Protect 11.1 to build and manage a Recovery as a Service (RaaS) offering.

PlateSpin Protect is a NetIQ disaster recovery product. It uses a VMware cluster as the target platform for replication of one or more source servers that need protection against disasters or power outages. These source servers can be physical or virtual Windows and Linux systems. Once the protection has been set up, the systems are replicated into warm stand-by virtual machines (VMs) in the VMware cluster. In case of a disaster, the warm stand-by VMs are booted to ensure business service continuity. Once the original source servers have been rebuilt, the contents of the warm stand-by VMs can be replicated back to their original location.

For more information on PlateSpin Protect, visit [www.netiq.com/products/protect](http://www.netiq.com/products/protect).

## Why is “Recovery as a Service” a Special Use Case?

When using PlateSpin Protect for RaaS deployments, a Service Provider will typically service multiple customers, called “tenants” in this document. Because there are multiple tenants, it is necessary to segment the target VMware cluster to allow for what is often called “multi-tenancy”. In a nutshell, multi-tenancy means that one RaaS tenant should never be able to see or access any artifact (VM, network, storage) or configuration setting belonging to another tenant. In order to create a multi-tenant environment, PlateSpin Protect 11.1 allows Service Providers to set up specific user roles in the VMware infrastructure. These roles make it possible to configure the infrastructure so that non-administrative VMware users representing the tenants can perform the necessary PlateSpin Protect 11.1 related lifecycle operations in the VMware infrastructure, all in a completely segregated fashion.

Secondly, because of the commercial relationship between a Service Provider and the tenant, the Service Provider will often wish to brand all graphical user interfaces that will be operated by the tenant with his own branding. This may include UI colors, logos, or both. PlateSpin Protect 11.1 features white-labeling, which allows for such rebranding - even per tenant if so desired.

Finally, because RaaS often happens over the Internet, the available bandwidth between the source servers and the target protection platform can be a challenge. PlateSpin Protect 11.1 features two relevant enhancements that will be highlighted in this document: image-based replication seeding and per-workload MTU tuning.



## Multi-Tenancy in the VMware Back-End Infrastructure

### Reference Architecture Diagram

The diagram below shows the main architectural components of a multi-tenant RaaS setup with PlateSpin Protect 11.1.

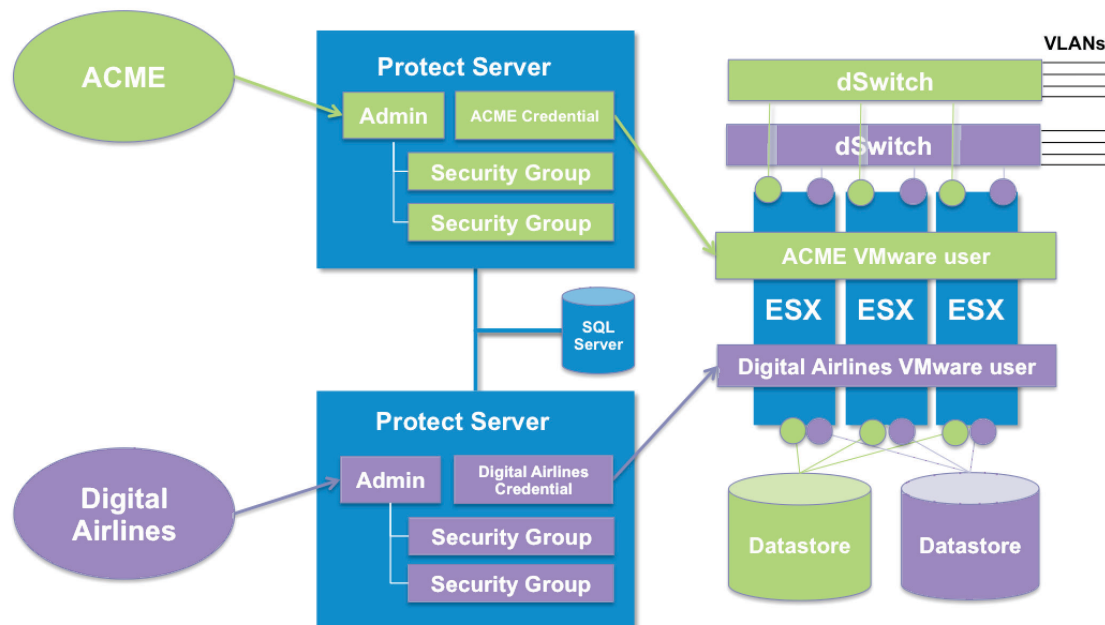


Figure 1 – PlateSpin Protect 11.1 Multi-Tenancy Reference Architecture Diagram

### Explanation of the Architectural Components

In this section, we'll use "ACME" and "Digital Airlines" as tenant names. Using PlateSpin Protect 11.1 for any kind of multi-tenant setup requires running one PlateSpin Protect server per tenant, so one for ACME and one for Digital Airlines. As a note, each PlateSpin Protect server is typically run in a single, dedicated virtual machine, since the service does not require a significant amount of resources. Although there are multiple PlateSpin Protect 11.1 servers, they can all use the same VMware cluster as the target for their respective replications.

The access that a PlateSpin Protect server has to a VMware cluster is defined by a credential. In a non-multi-tenant setup, it is safe to use a VMware administrative credential for accessing the VMware cluster. Using an administrative credential enables the Protect Server to see and use all resources in the VMware cluster (storage, networking, resource groups, virtual machines, etc.).

However, in multi-tenant setup, where there is one PlateSpin Protect server per tenant, administrative credentials cannot be used, since this would allow all tenants to see each other's assets in the cluster. The solution is to set up one non-administrative credential per tenant, in the form of a unique username and password combination. In the reference architecture diagram above, these credentials are called "ACME Credential" and "Digital Airlines Credential". These non-administrative credentials are created by the Service Provider in the VMware infrastructure. They are then used to set up the connection of the tenant's Protect Server to the VMware cluster (or "Container, in the PlateSpin Protect UI), but are never communicated to the tenant.



Each non-administrative credential corresponds to a VMware user in the VMware cluster. Each of these VMware users need to be linked to specific PlateSpin Protect generated roles (permission sets), for various objects in the VMware vCenter Datacenter view. The end result is a limited view of and/or usage of VMware datastores and networks: each tenant can only see and/or operate the objects that the Service Provider has given him/her permissions for.

At the same time each tenant can be given full administrative rights in his own PlateSpin Protect server. This is possible as the administrative credentials for the PlateSpin Protect server are not related to the non-administrative credentials for the VMware cluster. The administrative credentials for the PlateSpin Protect server can be shared with the tenant. This allows the tenant to set up multiple levels of visibility and/or management within his own Protect Server, by using PlateSpin Protect Security Groups. The privileges of each Security Group are limited by the privileges of the (secret) non-administrative VMware credentials.

## Defining the VMware Roles

NetIQ has created a file that defines the minimum required privileges for multi-tenancy and aggregates them into three distinct VMware roles:

- PlateSpin Virtual Machine Manager
- PlateSpin Infrastructure Manager
- PlateSpin User

This file, called `PlateSpinRole.xml`, is included in the PlateSpin Protect 11.1 server installation. An accompanying executable, called `PlateSpin.VMwareRoleTool.exe`, accesses the file and creates these custom PlateSpin Protect roles in the target vCenter environment. By default, the role definition file is located in the same folder which contain the role definition tool.

## Basic Command Line Syntax

From the location where the role tool was installed, run the tool from the command line, using this syntax:

```
PlateSpin.VMwareRoleTool.exe /host=[host name/IP address of the VMware vCenter server] /  
user=[user name] /role=[the complete path to the PlateSpinRole.xml file] /create
```

Note that the specified user needs to be a user with full administrative privileges in the VMware vCenter server. For a complete overview of the command line syntax of the role tool, and usage examples, consult the PlateSpin Protect 11.1 documentation on [www.netiq.com/documentation](http://www.netiq.com/documentation).



## Assigning the New Roles to Objects and Resources in vCenter

The following table specifies how to assign each non-administrative VMware user roles for the various containers in and artifacts in VMware vCenter. For all details on the configuration of the roles and the propagation instructions, consult the PlateSpin Protect 11.1 documentation on [www.netiq.com/documentation](http://www.netiq.com/documentation).

vCenter Container For Role Assignment	Role Assignment For Each Enabled User
Root of the vCenter inventory tree ("vcenterapp" in the images below)	<ul style="list-style-type: none"><li>• PlateSpin Infrastructure Manager</li><li>• Set to non-propagating</li></ul>
Each Datacenter to which the user needs access ("PlateSpin Datacenter" in the images below)	<ul style="list-style-type: none"><li>• PlateSpin Infrastructure Manager</li><li>• Set to non-propagating</li></ul>
Each cluster that will function as a PlateSpin Protect container and each host in that cluster ("Provo Cluster" in the images below)	<ul style="list-style-type: none"><li>• PlateSpin Infrastructure Manager</li><li>• Set to non-propagating</li></ul>
Each Resource Pool that is used by the user (e.g. "AMCE Protection" in the images below)	<ul style="list-style-type: none"><li>• PlateSpin User + PlateSpin Virtual Machine Manager</li><li>• Set to propagating</li></ul>
Each Folder where VMs belonging to the enabled user will be kept (e.g. "ACME VMs" in the images below)	<ul style="list-style-type: none"><li>• PlateSpin User + PlateSpin Virtual Machine Manager</li><li>• Set to propagating</li></ul>
Each Folder where tenant specific Networks, (d) vSwitches and (d)vPortgroups will be kept.	<ul style="list-style-type: none"><li>• PlateSpin Virtual Machine Manager</li><li>• Set to propagating</li></ul>
Each Folder where tenant specific Datastores and Datastore clusters will be kept.	<ul style="list-style-type: none"><li>• PlateSpin Virtual Machine Manager</li><li>• Set to propagating</li></ul>

Table 1 – PlateSpin Protect 11.1 Multi-Tenancy Reference Architecture Diagram



The images below show how the PlateSpin Protect roles need to be set in the vCenter UI.

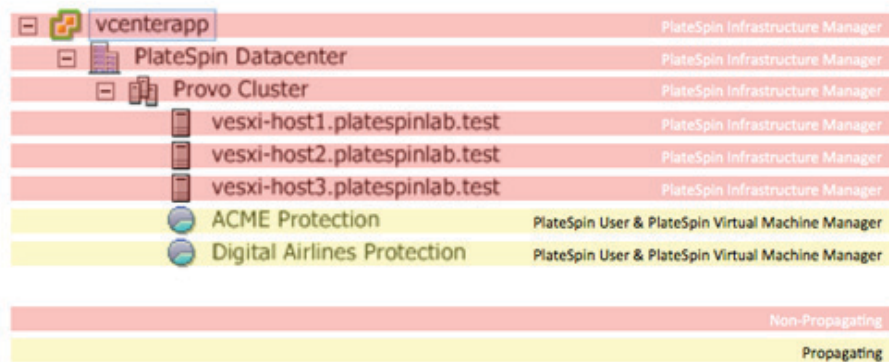


Figure 2 – Role Assignment for Datacenters, Clusters, Hosts and Resource Groups

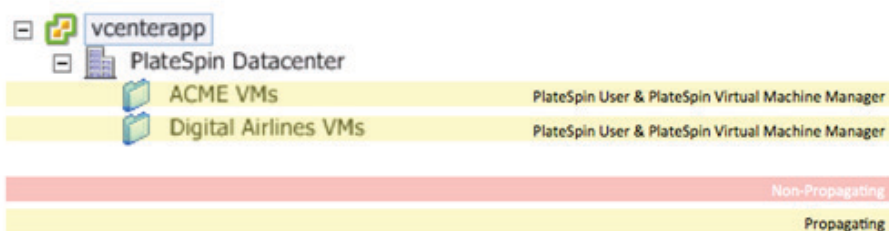


Figure 3 – Role Assignment for VM folders

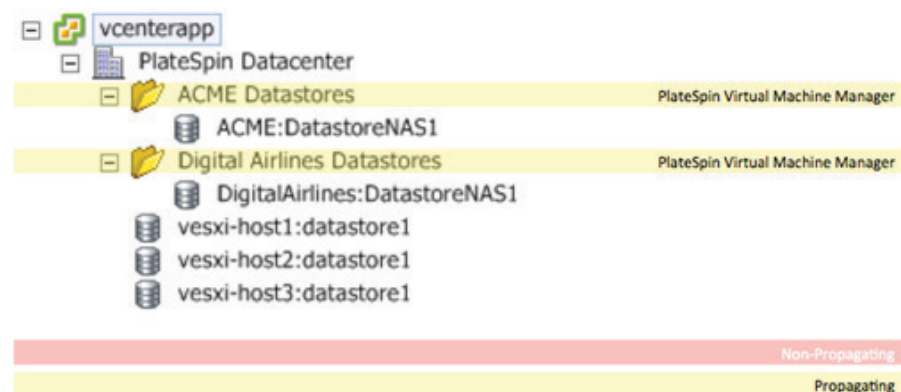


Figure 4 – Role Assignment for Datastore Folders

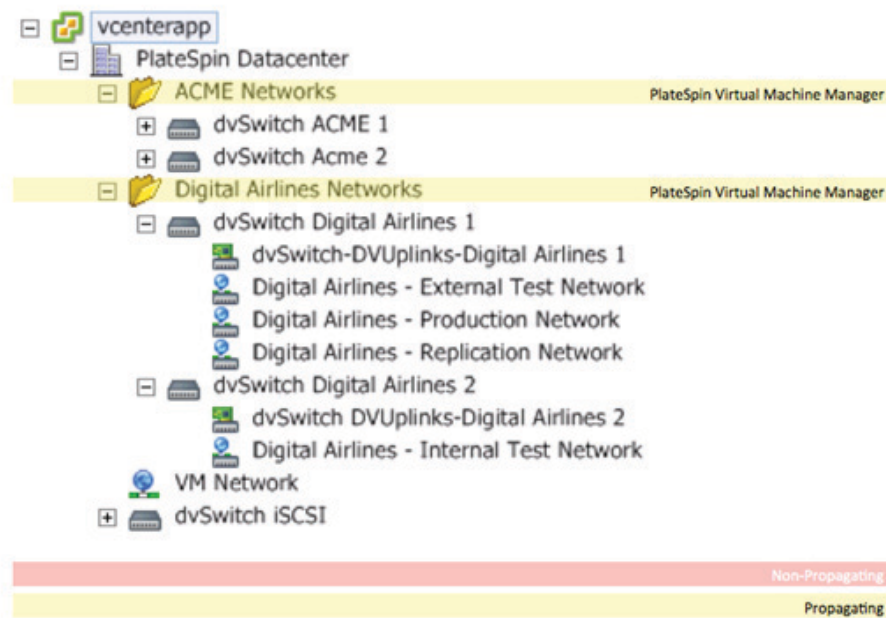


Figure 5 – Role Assignment for Network Folders





# Rebranding PlateSpin Protect 11.1

## High-Level Overview

There are many elements in the PlateSpin Protect 11.1 web interface that can be rebranded or customized. This can be done very easily by pointing your browser to [https://Your\\_PlateSpin\\_Server/platespinconfiguration](https://Your_PlateSpin_Server/platespinconfiguration). This page will display a set of parameters, some of which apply to rebranding and UI customization. To filter out the relevant items, type “webui” in the “Search” box in the upper left corner. This will give you a list of 12 configuration items. Each item corresponds to a specific UI setting. The images below visualize which setting applies to what UI widget.

### PlateSpin Server Configuration Settings

ID	WebUI Configuration Parameter and Description	Default Value
1	<b>WebUIFaviconUrl</b> Location of a valid .ico graphic file. Specify one of the following: A valid URL to the appropriate .ico file on a different machine. For example: <a href="https://myserver.example.com/dir1/dir2/icons/mycompany_favicon.ico">https://myserver.example.com/dir1/dir2/icons/mycompany_favicon.ico</a> A relative path below the root of the local web server where you have uploaded the appropriate .ico file. For example, if you create a path called mycompany\images\icons at the root of the web server to store your custom icon graphics: ~\mycompany\images\icons\mycompany_favicon.ico In this example, the actual file system path that contains the file is C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\icons\mycompany_favicon.ico.	~/doc/en/favicon.ico <sup>1</sup>  ~/Resources/protectLogo.png <sup>2</sup>
2	<b>WebUILogoUrl</b> Location of product logo graphic file. Specify one of the following: A valid URL to the appropriate graphics file on a different machine. For example: <a href="https://myserver.example.com/dir1/dir2/logos/mycompany_logo.png">https://myserver.example.com/dir1/dir2/logos/mycompany_logo.png</a> A relative path below the root of the local web server where you have uploaded the appropriate graphics file. For example, if you create a path called mycompany\images\logos at the root of the web server to store your custom logo images: ~\mycompany\images\logos\mycompany_logo.ico In this example, the actual file system path that contains the file is C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\mycompany\images\logos\mycompany_logo.png.	~/Resources/protectLogo.png <sup>2</sup>
3	<b>WebUIShowAboutTab</b> Toggle the visibility of the About tab on (True) or off (False).	True
4	<b>WebUIShowHelpTab</b> Toggle the visibility of the Help tab on (True) or off (False).	True
5	<b>WebUISiteAccentColor</b> Accent color (RGB hex value)	#0083CE
6	<b>WebUISiteAccentFontColor</b> Font color to display with accent color in Web UI (RGB hex value)	#FFFFFF
7	<b>WebUISiteBackgroundColor</b> Site background color (RGB hex value)	#666666
8	<b>WebUISiteHeaderBackgroundColor</b> Site header background color (RGB hex value)	#000000
9	<b>WebUISiteHeaderFontColor</b> Site header font color in Web UI (RGB hex value)	#FFFFFF
10	<b>WebUISiteNavigationBackgroundColor</b> Color of site navigation background in Web UI (RGB hex value)	#4D4D4D
11	<b>WebUISiteNavigationFontColor</b> Color of site navigation link font color in Web UI (RGB hex value)	#FFFFFF
12	<b>WebUISiteNavigationLinkHoverBackgroundColor</b> Color of site navigation link background in hover state (RGB hex value)	#808080

<sup>1</sup> Actual file path is C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\en\favicon.ico.

<sup>2</sup> Actual file path is C:\Program Files (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png.

Table 2 – PlateSpin Protect 11.1 UI Related Configuration Settings

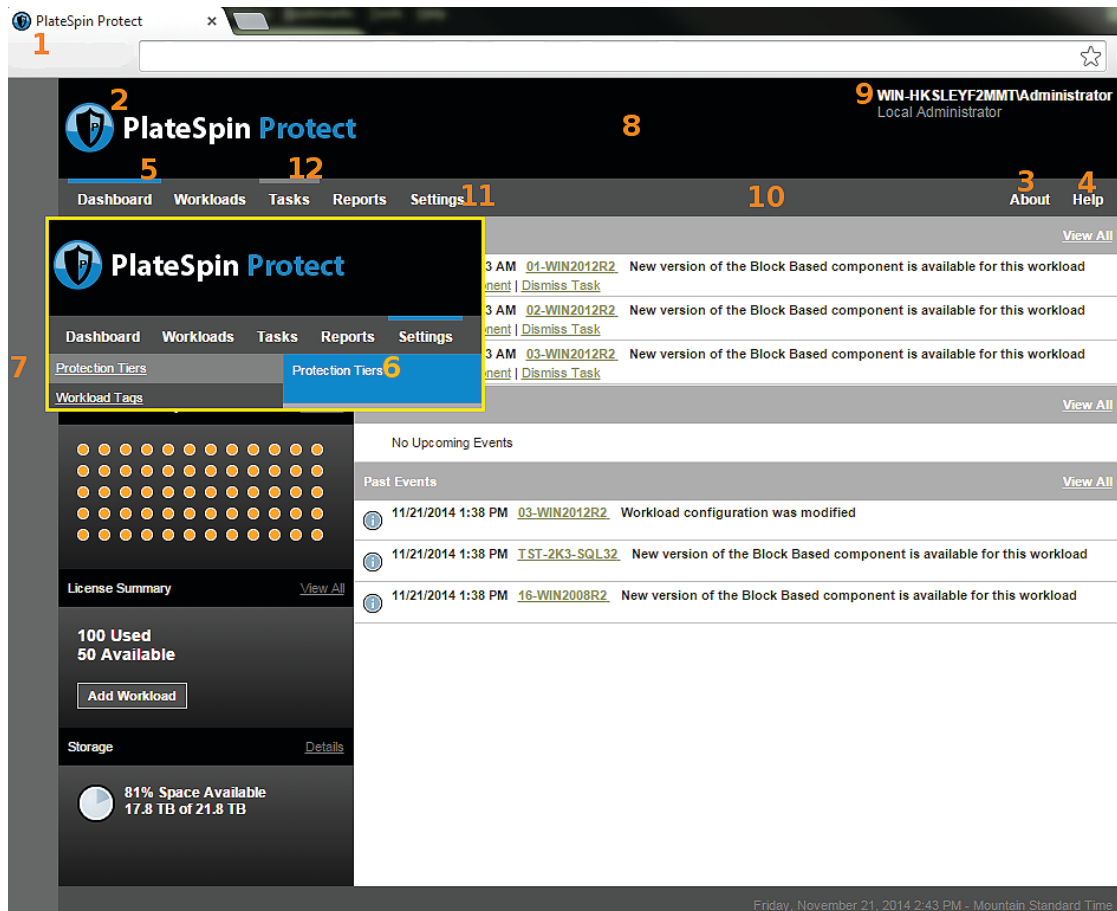


Figure 6 – PlateSpin Protect 11.1 Web UI



## Image-Based Replication Seeding

### High-Level Overview

PlateSpin Protect features a two-stage replication process. The first replication of a source server is always a “full” replication, which means that all blocks of the source workload are transferred to the target warm standby VM. After this first full replication, all subsequent replications are “incremental”. Incremental replications only contain the blocks that have been modified on the source server since the last full or incremental replication. The amount of blocks that needs to be transferred during an incremental replication depends heavily on the change rate of the source server, but is typically a lot less than for a full replication.

When operating over a network with low bandwidth, instead of performing the initial full replication over the network, the Service Provider may choose to first create an image of the source workload on-premise (or ask the tenant to do this), and then bring this image over to his data center. This can e.g. be done via a USB disk. Once the image is loaded up in the Protect Server, PlateSpin Protect can run a “Server Sync”, which tracks all the deltas that have occurred since the image was taken. After this initial Server Sync, standard incremental replications can be used to sync all subsequent deltas, just as if the first full replication was done over the network.

### Setup Procedure

1. In order to bootstrap the replication of a source server, a VMware OVF file of that source server needs to be created. When the source server is a VMware VM, a simple export into an OVF file is sufficient. Since exporting to an OVF file requires a power down, PlateSpin Migrate can be used to first create an exact copy of the source VM, which can then be powered off and exported. Similarly, when the source server is a physical system or a VM of another type than VMware, PlateSpin Migrate can be used to first convert the source system into a VMware VM, which can then be exported. For a detailed overview on how to use PlateSpin Migrate, consult the on-line documentation on [www.netiq.com/documentation](http://www.netiq.com/documentation).
2. Once an OVF file is obtained, transport this file to the target site, and import it into the desired PlateSpin Protect cluster. This cluster will function as the PlateSpin Protect container.
3. In the PlateSpin Protect UI, discover the source server and configure a PlateSpin Protect container for the VMware cluster in which you imported the OVF file.
4. In the PlateSpin Protect UI, set up a block-level Server Sync between the source server and the VM in the PlateSpin Protect container. This Server Sync will sync all the deltas between the source server and the target VM that happened since the OVF file was generated. This first synchronization is md5sum based and can take some time.
5. Once the Server Sync is done, set up incremental replication between the source server and target VM, using the desired Protection Tier.



## MTU Tuning for Replication Traffic

PlateSpin Protect contains many features that are beneficial on slow or unstable networks. As an example, NetIQ has implemented a fail-safe protocol on top of TCP, to cope with unexpected network outages and packet drops. It's also possible to compress the replication data that is sent over the network, in order to reduce the total load that needs to be sent.

In PlateSpin Protect 11.1, the latest addition is the ability to specify the TCP/IP MTU (Maximum Transmission Unit) for each server replication. Tuning the MTU can help to avoid jabber over networks that have smaller MTU values, e.g. when a VPN is used. On these networks, data packets with an MTU that is too high will typically be split into smaller packets. This process can dramatically increase the replication time. By reducing the size of the MTU so that it matches the smallest MTU on the network between the source server and the target VM, this splitting of packets is avoided.

Tuning the MTU can easily be done in the PlateSpin Protect 11.1 UI, as shown in the screen shot below. The default value is an empty string (nothing listed in the text box). This allows the replication network interface to set its own default (which is usually 1500). If a value is provided, PlateSpin Protect 11.1 adjusts the MTU while configuring the network interface.

Replication Settings

Transfer Method:

- ☐ File Based
- ☒ Block Based
  - ☒ Use components
  - ☐ Do not use components
- ☐ Encrypt Data Transfer

Source Credentials:

User Name: domain\Administrator

Password: [masked]

[Test Credentials](#)

Credentials Passed

Number of CPUs: 1

Replication Network:

Replication Network

☒ DHCP ☐ Static MTU:

Allowed Networks:

Allow	Name	Address	Uses DHCP
<input checked="" type="checkbox"/>	Ethernet	192.168.1.150	False

Configuration File Datastore: forge:datastore1 (20.5 TB free)

Protected Volumes:

Include	Name	Used Space	Free Space	Datastore	Thin Disk
<input checked="" type="checkbox"/>	C: (NTFS - Boot)	7.8 GB	31.88 GB	forge:datastore1 (20.5 TB free)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	\\?\Volume{73183d8d-4db5-11e4-80b1-806e6f6e6963} 260.9 MB (NTFS - System)		89.13 MB	forge:datastore1 (20.5 TB free)	<input type="checkbox"/>

Figure 7 – PlateSpin Protect 11.1 Multi-Tenancy Reference Architecture Diagram



## Multi-tenancy for Microsoft SQL Server 2014

Multiple PlateSpin Protect 11.1 servers can share the same instance of Microsoft SQL Server. Using one instance of SQL Server reduces licensing and operations costs, and can lead to increased security because only one instance has to be monitored and maintained.

PlateSpin Protect 11.1 supports both SQL Server Authentication and Microsoft Windows Authentication. However, for a multi-tenant database setup Microsoft Windows Authentication is required: a multi-tenant setup requires one Microsoft domain account with the SQL Server system administrator “sysadmin” role, and then one dedicated domain account for each PlateSpin Protect server.

When installing SQL Server 2014, configuring any Microsoft domain account as a SQL Server system administrator can easily be done as part of the setup, as shown below:

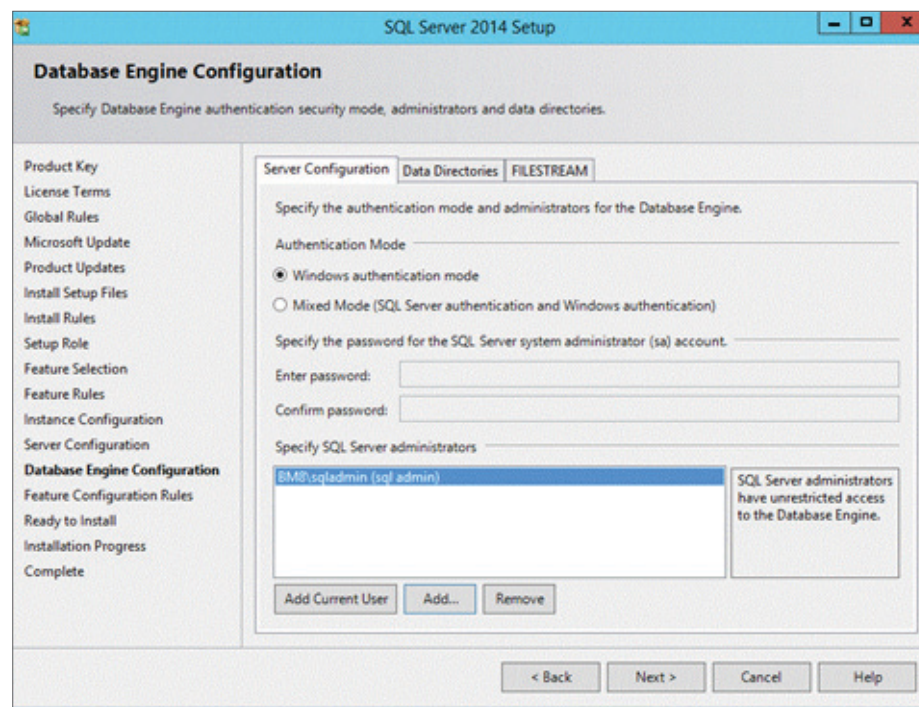


Figure 8 – Setting up a SQL Server System Administrator using a domain account

After the SQL Server is installed, one or more PlateSpin Protect servers can be installed. While installing each PlateSpin Protect server, the installation wizard will ask for the credentials of the SQL Server system administrator, as well as credentials for a Database Service User. This Database Service User should be a dedicated domain account with limited domain permissions, but has to be local administrator on the Microsoft Windows Server on which you are installing PlateSpin Protect. The credentials of the SQL Server system administrator are used to create new databases in the SQL Server instance, after which the Database Service User is granted rights to these databases. For multi-tenancy purposes, NetIQ recommends to create at least one unique Database Service User per RaaS customer. Should a customer need multiple PlateSpin Protect servers, then the same Database Service User can be used for all of their PlateSpin Protect servers.

In the context of multi-tenancy, it's important to stress that the credentials of the SQL Server system administrator are never stored on the PlateSpin Protect Server.



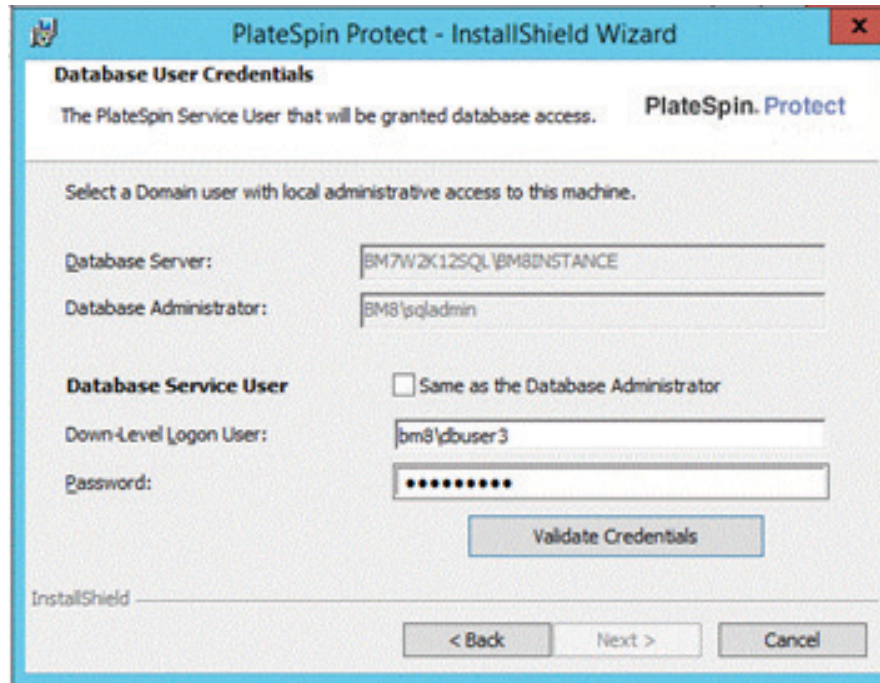


Figure 9 – Setting up the Database Service User while installing PlateSpin Protect 11.1



## About NetIQ

NetIQ is a global, IT enterprise software company with relentless focus on customer success. Customers and partners choose NetIQ to cost-effectively tackle information protection challenges and manage the complexity of dynamic, highly-distributed business applications.

Our portfolio includes scalable, automated solutions for Identity, Security and Governance, and IT Operations Management that help organizations securely deliver, measure, and manage computing services across physical, virtual, and cloud computing environments. These solutions and our practical, customer-focused approach to solving persistent IT challenges ensure organizations are able to reduce cost, complexity and risk.

To learn more about our industry-acclaimed software solutions, visit [www.netiq.com](http://www.netiq.com).

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Copyright © 2014 NetIQ Corporation and its affiliates. All Rights Reserved.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

### Worldwide Headquarters

505 Post Oak Blvd., Suite 1200  
Houston, Texas 77027 USA  
Worldwide: +713.548.1700

**U.S. / Canada Toll Free:** 888.323.6768

[info@netiq.com](mailto:info@netiq.com)

[www.netiq.com](http://www.netiq.com)

<http://community.netiq.com>

### For a complete list of our offices

In North America, Europe, the Middle East  
Africa, Asia-Pacific and Latin America,  
please visit [www.netiq.com/contacts](http://www.netiq.com/contacts).