Technical Review

Four Critical Benefits of Automating Disaster Recovery with Veeam Availability Orchestrator

Date: November 2019 **Authors:** Vinny Choinski, Senior IT Validation Analyst; and Christophe Bertrand, Senior Analyst
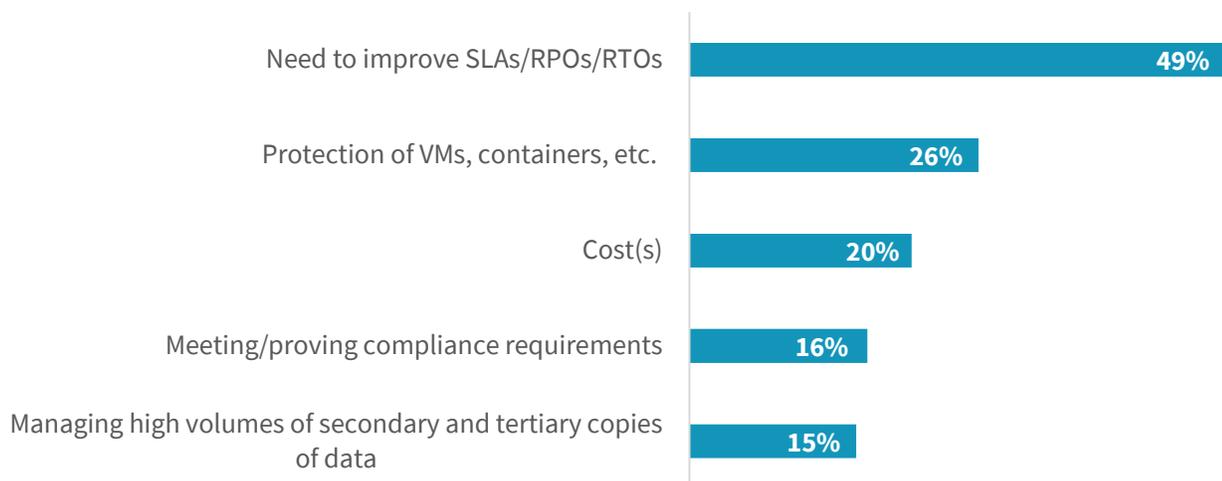
Abstract

This ESG Technical Review documents hands-on validation of Veeam Availability Orchestrator. The goal of the report is to validate that the solution supports business continuity/disaster recovery (BC/DR) in a variety of failure scenarios, enhancing the business's ability to create accurate and reliable recovery plans while significantly reducing the effort required to test, validate, and execute these plans.

The Challenges

ESG research reveals that businesses identified improving SLAs and reducing RPOs and RTOs as top challenges when looking at their data protection technologies and processes.[1] Businesses are increasingly relying on their IT systems to deliver critical business functions in a 24x7x365 manner. Critical applications that support these functions need to be recoverable quickly and reliably in a variety of different failure scenarios including component failure, data corruption, ransomware attacks, and the failure of an entire data center. However, today's modern applications are more complex, distributed, and interdependent, making the successful recovery of even a single application challenging, as many dependent tasks must be performed in a specific sequence and without error. Multiply this by the hundreds of applications that the IT organization must support, and the scope of the problem becomes insurmountable. It's clear that trying to manually create, maintain and execute against runbooks is error-prone, labor-intensive, and difficult to test and validate. Businesses just don't have the resources to operate this way today, making orchestration and automation of backup and recovery processes an indispensable tool.

Figure 1. Data Protection Challenges

Which of the following would you characterize as the top challenges with your organization's current data protection processes and technologies?

Need to improve SLAs/RPOs/RTOs	49%
Protection of VMs, containers, etc.	26%
Cost(s)	20%
Meeting/proving compliance requirements	16%
Managing high volumes of secondary and tertiary copies of data	15%

Source: Enterprise Strategy Group

---

[1] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.

The Solution: Veeam Availability Orchestrator

Veeam Availability Orchestrator (VAO) is a reliable, scalable, and easy-to-use orchestration and automation engine that's purpose-built for today's BC/DR needs. By automating the process of creating, documenting, testing, and executing disaster recovery (DR) plans, it helps organizations maintain business continuity and compliance while eliminating manual processes that are inefficient, lengthy, and error prone. Full orchestration and automation support is also extended to restores from backups, enabling DR practices to be extended to all applications and data across the organization, not just those deemed mission-critical.

ESG Validated

ESG performed hands-on evaluation of Veeam Availability Orchestrator in Veeam's demo environment. Key elements of the environment included: source and target VMware vSphere environments including vCenter, a Veeam Backup & Replication server with existing backup images and datastore replicas, the VAO server, and a DataLabs proxy appliance. The validation process involved creating a new VAO recovery plan, testing and monitoring the plan as the infrastructure came on-line in the isolated environment, a review of the automated documentation, and then a real-world execution of the plan.

The key solution benefits ESG validated include:

- **Reliable, application-centric recovery:** Not all applications are created equally when it comes to recovery processes, or the SLAs required by the business. VAO allows recovery plans to be built on business logic that is defined at the application-level where appropriate to ensure they are recovered quickly and reliably the first time, while prioritizing those that are more critical.
- **Flexible DR using replicas and/or backups:** Orchestrated recovery from replicas or backups allows organizations the flexibility to choose a method of data protection that suits specific SLAs. This enables them to apply a comprehensive DR toolset to a broader set of applications while also reducing costs.
- **Fully automated testing and validation:** Automated testing of DR plans in a non-disruptive environment ensures that plans can be validated frequently and thoroughly without requiring the time or cost of legacy manual methods. This also ensures errors are highlighted early and addressed proactively.
- **DR documentation and compliance.** The automated reports contain a continuous log of plan changes that helps users stay on top of constantly changing applications. They also include detailed testing and recovery outcomes that are ideal for proving compliance—another organizational top challenge highlighted in Figure 1.

Getting Started with Veeam Availability Orchestrator

As shown in Figure 2, installing VAO involves deploying and configuring the VAO server through a wizard-driven process. Because the VAO server is required to execute the orchestrated recovery plans, it is typically installed at a remote site (e.g., a DR site), which usually also serves as a target for recovered applications. The VAO server is where all configuration, administration, and management functions are performed in addition to being where all orchestration events are executed. A VAO agent must be installed on existing Veeam Backup & Replication servers, and the VAO server requires access to all vCenter Servers that are in either the production or DR site.

Figure 2. VAO Architecture Overview
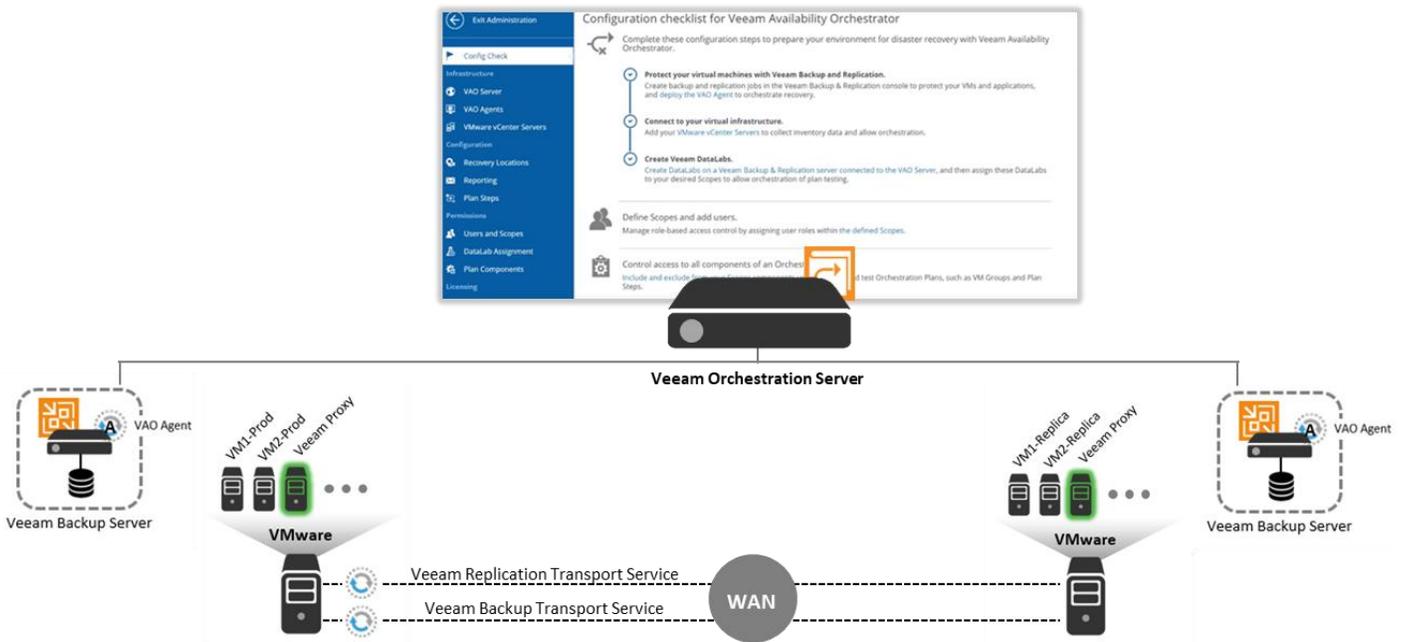
Configuration of Veeam Availability Orchestrator

ESG started the evaluation process by connecting and logging in to the VAO server via the web-based UI. From the main menu, as shown in the first image in Figure 3, we were able to review key elements of the solution that require configuration, such as the vSphere environments that were configured to VAO, the Veeam Backup & Replication servers running the VAO agent, the DataLabs testing environments that were known to VAO, the various reports that were available, user and scope definitions, and the defined plans and plan steps.

Figure 3. VAO Configuration of Recovery Sites, Users, and Scopes
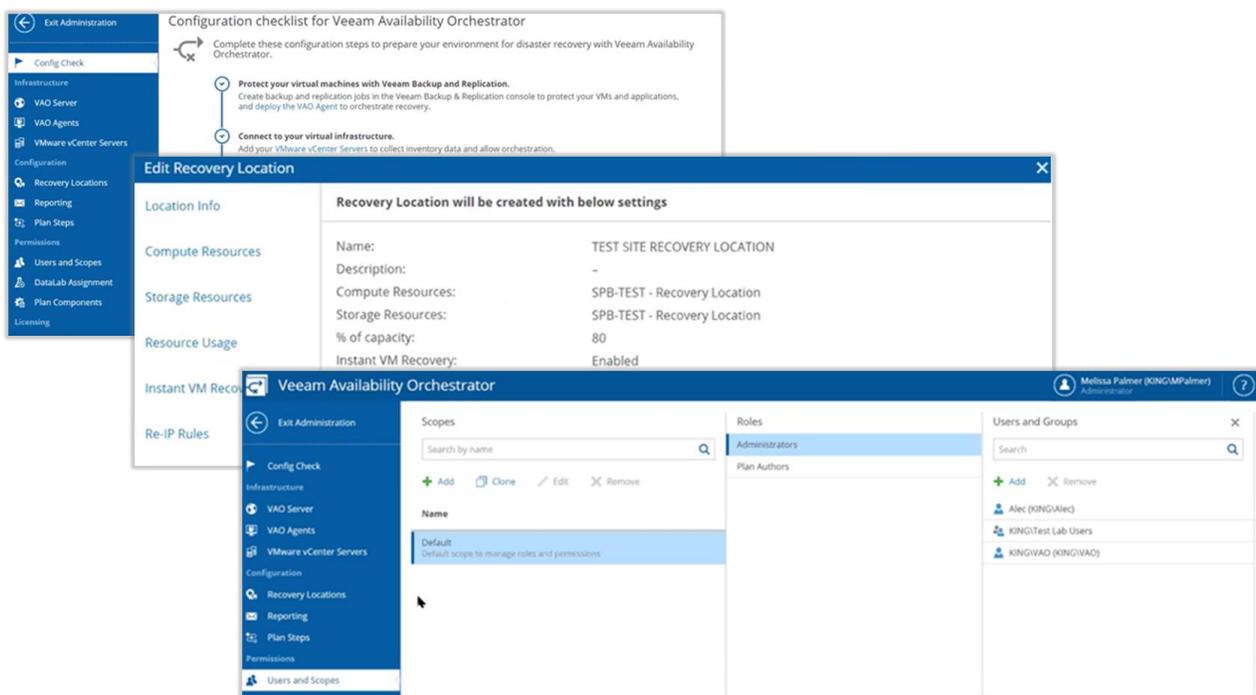
As shown in Figure 3, ESG reviewed and defined all recovery locations. The recovery locations represent the locations where VMware vSphere infrastructure exists that will be the target for recovery plans. In a typical implementation, the recovery location would be a remote DR site for a production data center, or it could also be the production data center for a ROBO location. In the definition of the recovery site, you can also control what happens from an IP configuration perspective, for example, enabling IP addresses to be reconfigured or not.

Another configuration option when leveraging VAO is whether to orchestrate recovery using replicas or backups. When orchestrating restores from backups, users can select the "Instant VM Recovery" option, allowing virtual machines (VMs) to be started directly from the backup file(s), helping speed up the process of bringing VMs on-line once all prerequisite recovery plan steps have completed.
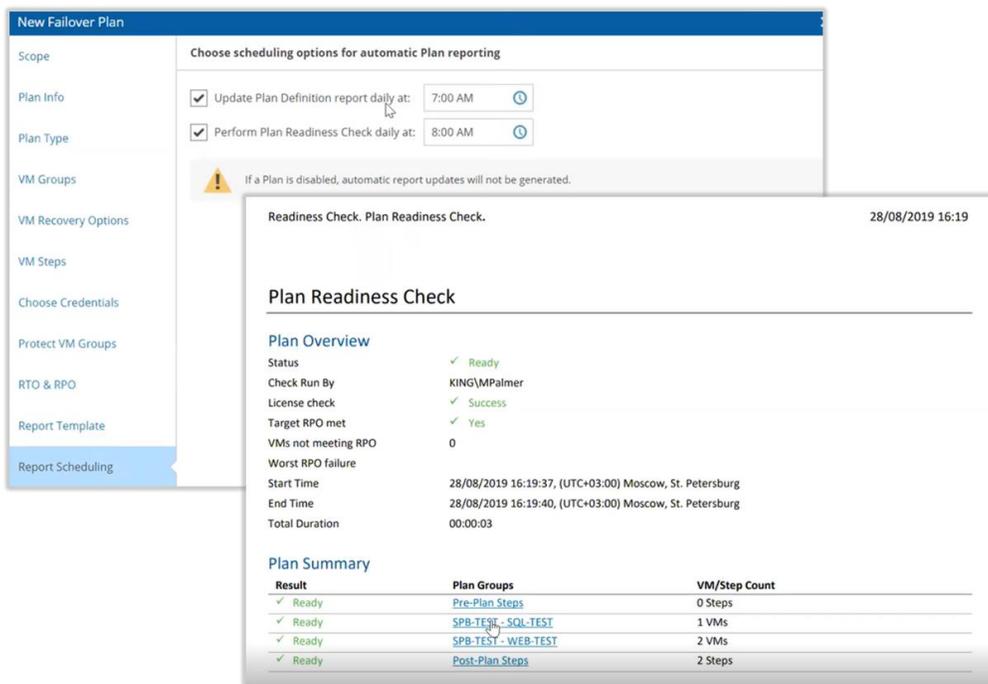
Why This Matters

The ability to orchestrate recovery from both replicas and backups within VAO presents users with multiple options when planning for DR. Not all applications are created equally and as such, not all applications require the low RPOs and RTOs offered by replication; however they still need to be brought on-line quickly and efficiently in the event of outage. VAO empowers users with the flexibility to opt for data protection methods that best suit the needs of the application while still offering the benefits of orchestration and automation. Furthermore, utilizing Instant VM Recovery when restoring from backups helps cut RTOs, even when replication isn't used or viable.

We then reviewed the configuration of users, roles, and scopes. Scopes are used to control user access to specific functionality, including operations users can perform and what data and resources they can access. Scopes are useful configuration settings that align users and roles with relevant business constructs, such as specific organizations or organizational roles.

Next, we reviewed how reports are defined and associated with recovery plans and scopes. There are four kinds of reports automatically generated by VAO:

- The *Definition Report* provides a detailed look at a recovery plan and tracks changes made to the plan.
- The *Readiness Check Report* checks the recovery plan against the target recovery environment. No actual recovery or failover takes place.
- The *Test Execution Report* contains the details of a test recovery in a DataLab environment, providing the results of the test like achieved RTOs and RPOs, and the configured test environment.
- The *Execution Report* contains the detailed results of the execution of a recovery plan and includes the state of the recovered VMs and any errors that were encountered during plan execution.

Figure 4. VAO Configuration of Recovery Sites, Users, and Scopes


Why This Matters

ESG's research shows that a top challenge for businesses is meeting the SLAs/RPOs/RTOs of their critical business applications. Manually tracking application and infrastructure changes, updating runbooks, assessing how the changes impact recovery plans, and then testing and documenting outcomes is no longer a workable solution for businesses. ESG confirmed that VAO automates this entire process and provides actionable reports on the status of the recovery plans.

The role-based access controls and scopes within VAO empowers business stakeholders to take a more proactive role in ensuring that the business's critical applications can be recovered when failure occurs. The *Plan Definition* and *Plan Readiness* Reports can be scheduled to run daily, and the results can be delivered to all stakeholders. This ensures that any changes to the application's infrastructure and data protection configuration that might impact recoverability are addressed proactively in a timely manner.

Building Comprehensive, Customizable Orchestration and Automation Plans

Once we completed a review of the VAO configuration, including the recovery sites, scopes, and reports, we moved on to creating a recovery plan. And because we wanted to watch an actual recovery taking place (via vCenter), we created a recovery plan that would leverage a Veeam DataLabs target environment. With Veeam DataLabs, the recovery environment is brought on-line without having to make changes to IP addresses, DNS entries, Active Directory, etc., because it is totally isolated from the source/production environment.

As shown in Figure 5, we began the process of building a new plan by giving the plan a name, "ESG Review," and description. We then had to select the type of plan we were creating. For our test plan, we selected a Failover Plan type. We then selected the VM Groups for the VMs that would be included in the plan. VM Groups are not managed within VAO but rather from within VMware vCenter via tags or Veeam ONE Business View. VM groups can be created and managed in multiple ways, including tagging from within vCenter, and are often used to organize VMs to align with groupings that make sense to the business.

Figure 5. Building a New Orchestration Plan
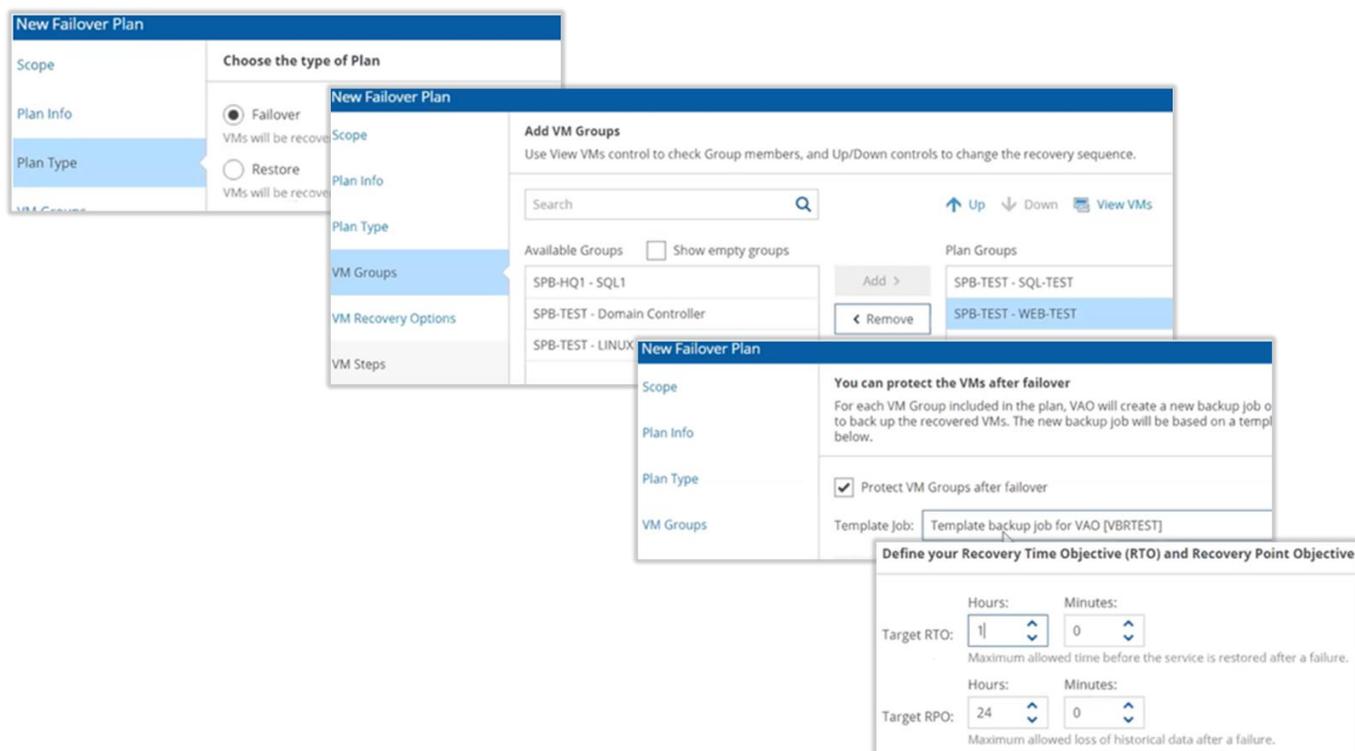
During plan creation, we were also able to customize other important parameters including the required RPO and RTO. VAO lets you know if the specific RPO is achievable based on the available replica and backup data. The user can also select parallel or serial recovery of VMs and, with parallel recovery, how many VMs to recover simultaneously. VAO enables the user to decide whether to keep the VMs up after they are recovered or to shut them down at the end of the test, and whether or not to begin protecting the VMs after they are started with Veeam Backup & Replication. It should be noted that many of these processes are canned steps built into VAO. In addition to the built-in VAO plan steps, users can achieve virtually anything with the ability to define custom plans steps. These are easily added by uploading a PowerShell script to VAO, like ones that may already be in use when manually executing DR. These custom plan steps can also be executed out-of-band and don't need to be run against the servers being recovered. A good example of this would be a PowerShell script that makes the necessary DNS changes in the event of disaster.

> ## ⓘ Why This Matters
>
> VAO allows businesses to create, manage, and monitor very detailed and customized recovery plans for data center applications. This customization is key because each application can have unique prerequisites, dependencies, and post-recovery operations that must take place for recovery to be successful.
>
> Creating a recovery plan is simple via the VAO UI with many predefined recovery steps available for inclusion. In addition, the ability to add any custom PowerShell-based scripts into the recovery plan enables virtually unlimited flexibility for the business.

Automatically Testing and Executing the Plan

Finally, ESG tested the Failover Plan, leveraging an isolated Veeam DataLabs target environment at the recovery site. Prior to testing the plan, we ran both the *Plan Definition* and *Readiness Check Reports* to ensure we had a clean plan that was free from errors. This is important because it provides a quick mechanism to ensure that the plan was built properly without having to go through multiple failure scenarios while testing. This has the potential to save lots of time by eliminating errors that wouldn't have been identified until a full application recovery test was performed.

Through the VAO management interface, we were able to initiate and follow the execution of the failover. Doing so was as simple as selecting Failover and inputting credentials. We were also able to monitor the state of the VMs as they booted and came on-line via vCenter. As you can see in Figure 6, the status of each step is shown along with details of the step as it is executing. In this case, you can see that we are waiting for a domain controller (DC) to boot before moving on to the following step, "Check VM Heartbeat." The remainder of the recovery completed successfully and without incident.

Figure 6. Orchestration Plan Execution
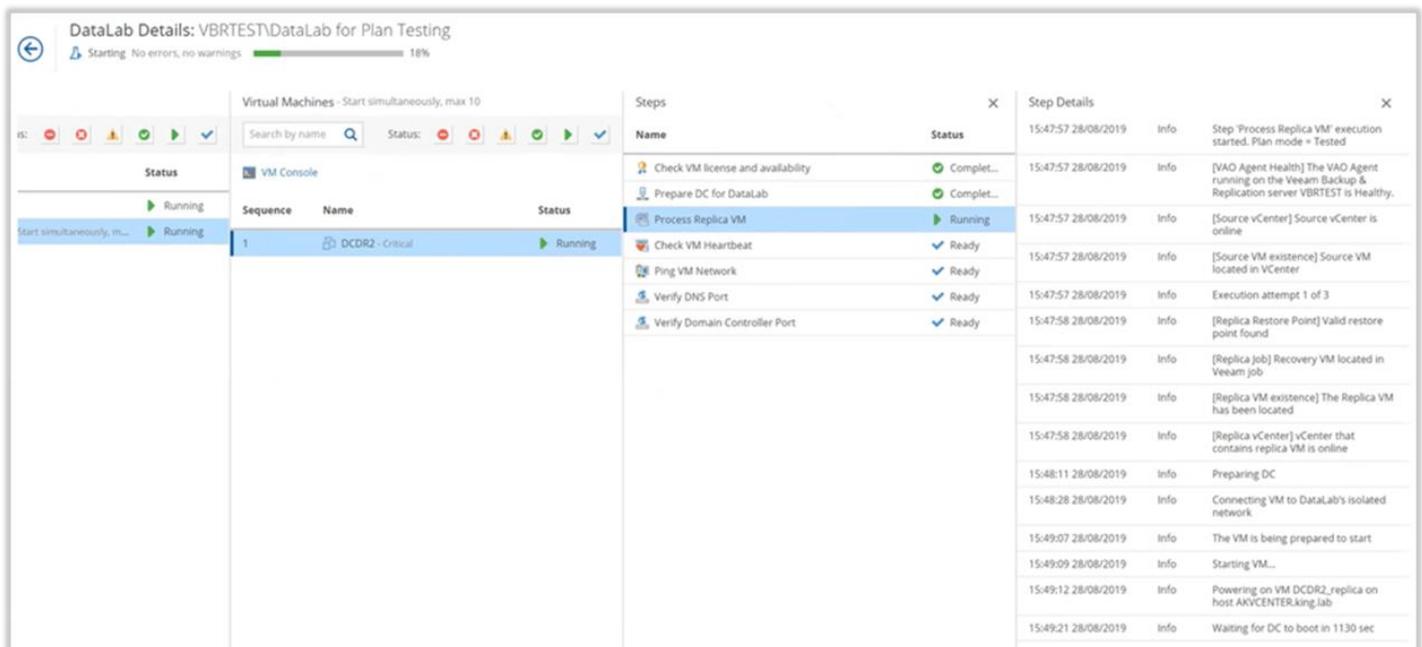
Why This Matters

The ability to leverage isolated Veeam DataLabs to perform fully-automated recovery tests that replicate the active production environment while minimizing the impact on the production environment enables the business to test its recovery plans more frequently, with greater success and less effort. This ensures that applications can be recovered in a manner that meets the business's SLAs and satisfies regulatory compliance requirements.

These isolated copies of the production environment can also be left powered-on upon completion of the test failover or recovery. This extends the uses of VAO beyond DR to IT Operations and Application Development Teams as testing, development, and analytics can be safely and securely performed against production-fresh data non-disruptively and non-destructively.

The Bigger Truth

For many businesses, 24x7x365 availability of applications has become the norm rather than the exception. Applications must be "always-on" to support the business's more demanding SLAs. The pace of accelerated application development and rollout means that IT Operations must have the ability to non-disruptively deliver the test, QA, and user-acceptance environments that align with the business's goals. In many cases, a self-service capability is required to properly service the Development Team. But, for most businesses, the IT Operations staff is not expanding, despite these increasing service demands. VAO helps IT Operations better meet this need.

Veeam Availability Orchestrator delivers on its promise of giving businesses a flexible, comprehensive and easy-to-use mechanism for creating orchestrated recovery plans that scale from the recovery of a single application to an entire data center. This new version of VAO adds to previous capabilities by allowing Veeam Backup & Replication backups to be used as the source for recovery plans. While VAO's core mission is to allow businesses to easily create, manage, test, and validate application recovery plans in the event of a business outage, the reality is that these same capabilities address other use cases for both the IT Operations and Application Development Teams.

VAO also helps businesses address the increase in IT infrastructure and application complexity that is taking place in most businesses. For businesses of all sizes, traditional, manual techniques for managing application availability and resiliency are no longer adequate. VAO allows current IT staff to develop, manage, and validate BC/DR plans without having to develop new skill sets. And with the use of RBAC and scopes, VAO can break down the typical organization barriers that exist between the business's various stakeholder organizations, creating a more integrated approach to BC/DR and then resilience and management of IT.