

Checklist for VPs Responsible for Business Service Management

Manage, secure, and optimize availability and performance of business services.

As the VP responsible for business service management for your company, you know that having an accurate, up-to-date CMDB is critical to success. You need to ensure that your team has what it needs to:

- Ensure complete discovery and dependency mapping for the CMDB
- Enable continuous CI dependency discovery
- Optimize the use of scanning and agents for maximum productivity and minimum impact on performance

This checklist provides you an overview of the key capabilities your team needs to meet these goals.

Accurate, complete discovery and dependency mapping

- Complete initial discovery.
 You need to identify all the CIs on your network and their dependencies to provide an accurate and up-to-date inventory for your CMDB.
- Complete CI dependency mapping.
 Discovery based on scanning provides “snapshots” that will miss much of the actual application-to-server and server-to-server dependencies that exist in your data center. In order to achieve an “as is” CI dependency map, you need to incorporate flow-based discovery methods that can passively capture data 7x24 without affecting network or server performance.
- Avoid credential and performance problems.
 Scanning approaches have several limitations. Certain systems aren’t available to scanning due to firewalls and/or network configuration or credential issues. Pervasive scanning can also create performance problems. You need to be able to supplement such approaches with technologies that passively acquire the data you need.

Continuous CI dependency discovery

- Continuous collection of CI and dependency data.
 You need to be able to collect flow-based data about CIs and their dependencies, including changes, and export that data on a scheduled basis to ensure that your CMDB is always accurate.
- Avoid coverage or time gaps.
 You need to ensure that your data collection is continuous and complete to ensure that updates made to the CMDB accurately reflect the use of business services.

Optimized use of scanning and agents

- Optimize scanning.
 You need to ensure that all systems that should be scanned are being scanned and that new scanning candidates are being appropriately selected based on the system’s relative importance to the delivery of key business services. Flow-based discovery enables you to get information for all systems and use scan-based discovery for only those systems where it is needed; this minimizes performance impact and effort required to secure access credentials.
- Avoid performance hits.
 Use a passive discovery approach for broad coverage to avoid the performance hit and limitations of scanning. This enables you to focus the use of scanning where and when it is most needed.
- Optimize use of agents in the data center.
 The data center’s dynamic nature can result in servers without appropriate coverage. You need to be able to automatically identify hosts in the data center and apply agents as appropriate to accurately assess those assets.
- Optimize use of agents outside the data center.
 Many critical assets exist outside of the data center; you need to be able to identify these assets, enabling you to apply the appropriate level of identification and management to the assets.

For more information on how Mazu Profiler Discovery provides a new way to passively discover configuration items and their dependencies across the entire enterprise to support these capabilities, please contact your Mazu sales representative or go to www.mazunetworks.com.