Foundation and CloudScape
User Guide
Legal Information

Book Name: Foundation and CloudScape User Guide
Part Number: FCS-29MARCH2021-UG01
Product Release Date: 29 March 2021

Copyright Notice

Copyright © 2021 Flexera Software
This publication contains proprietary and confidential information and creative works owned by Flexera Software and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera Software is strictly prohibited. Except where expressly provided by Flexera Software in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera Software intellectual property rights, whether by estoppel, implication, or otherwise.
All copies of the technology and related information, if allowed by Flexera Software, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see https://www.flexera.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.
Contents

1 Foundation and CloudScape User Guide ................................................................. 9
   Product Support Resources ...................................................................................... 10
   Contact Us ................................................................................................................ 11

2 Foundation and CloudScape Overview ................................................................. 13
   Architecture, Data Handling, and Security ............................................................. 13
      Foundation and CloudScape Architecture ......................................................... 14
      RN150 Virtual Appliance Security ..................................................................... 14
      Data Confidentiality and Compliance ............................................................... 16
   Advanced Debugging ............................................................................................... 16
   Multifactor Authentication ...................................................................................... 17

   What We Collect ..................................................................................................... 19

   How We Collect ..................................................................................................... 24
      Windows Collection Module ............................................................................... 26
         WMI .................................................................................................................. 26
         Remote Commands ......................................................................................... 28
         Windows Collection Module Troubleshooting .............................................. 30
         Windows Collection Module References ...................................................... 31
      SSH Collection Module ..................................................................................... 31
         SSH Collection Module Overview ................................................................. 32
         Supported Operating Systems ....................................................................... 32
         System Eligibility ............................................................................................. 32
         Credential Utilization ....................................................................................... 33
         User Account Requirements ........................................................................... 33
         Authentication Types ......................................................................................... 34
         Key-Based Authentication Requirements ....................................................... 34
         Privilege Elevation ............................................................................................. 34
         Entering Credentials ......................................................................................... 35
         Custom Server Ports ......................................................................................... 36
Contents

Configuration Examples .......................................................... 37
Creating a User Account On Linux ........................................... 37
Creating A Key Pair ............................................................ 38
Testing Sudo Configuration ..................................................... 38
Basic Example Sudo Configuration .......................................... 39
Advanced Example Sudo Configuration ................................. 39
SSH Collection Module Command Reference ............................. 39
SSH Collection Module Linux Command Reference ................... 40
SSH Collection Module AIX Command Reference ....................... 44
SSH Collection Module Troubleshooting ................................. 46
Troubleshooting Introduction .................................................. 46
Troubleshooting Command Reference ....................................... 47
Troubleshooting Command Suite ............................................. 48
SSH Collection Module Error Messages ................................. 50
Database Module ............................................................... 52
Overview of the Database Module ........................................... 52
Using the Database Module .................................................... 53
Queries Run By the Database Module ...................................... 54
Load Balancers .................................................................. 56
AWS Collection Module ......................................................... 56
Performance Counter Disambiguation ..................................... 58
Disambiguation / Clarification on Selected Counters .................. 58
Data Sources .................................................................. 59
Sampled vs. Aggregate Data ................................................... 60
ServiceNow Configuration and User Guide ............................ 60
ServiceNow Plugin Introduction .............................................. 60
Configuring and Setting Up the Plugin .................................... 61
Importing the Plugin in ServiceNow ......................................... 62
Uninstalling the Plugin .......................................................... 63
Creating a User ................................................................ 66
Providing Roles to a User ........................................................ 67
Connecting to External Systems ............................................. 69
Configuring RISC Networks Credential ................................. 69
Testing the Configuration ....................................................... 71
RISC SNOW Workflows ........................................................ 71
Discoverable Devices ............................................................. 71
Viewing the SNOW Workflows .............................................. 73
Listing Devices ................................................................ 74
Adding Tags ................................................................ 75
Viewing the Relationship ....................................................... 77
CI Relationship ................................................................ 80
Viewing Existing CI and RISC CI Relationship ......................... 80
Creating Relationship Manually ............................................. 81
Support and Troubleshooting .................................................. 83
Viewing Logs ................................................................ 83
Setting Log Level ................................................................ 84
## Contents

Overview of Appliance NTP Support ................................................................. 171
Configuring NTP on the Virtual Appliance .................................................. 172
NTP Configuration Values ........................................................................... 173

### 3 Getting Started with Foundation and CloudScape .................................. 175

#### Predeployment Checklist ........................................................................ 175

**Quick Start Guide** .................................................................................... 176

- Prerequisites ......................................................................................... 177
- Create an Assessment ............................................................................ 177
- Deploy the RN150 .................................................................................. 178
- Log In to the RN150 ............................................................................... 178
- Enter Your Assessment Key .................................................................... 179
- Enter Subnet Information ........................................................................ 179
- Enter SNMP Information ........................................................................ 180
- Enter Windows Credentials ..................................................................... 180
- Enter VMWare Credentials ..................................................................... 181
- Enter SSH Credentials ............................................................................ 181
- Additional Credentials ............................................................................ 182
- Additional Features ................................................................................ 182
- Complete Bootstrap and Start Scan ......................................................... 183
- Review Assets and Request Rescan ......................................................... 183
- License Devices for Data Collection ......................................................... 184
- Next Steps ............................................................................................. 184

**Discovery: How To** .................................................................................. 185

- Understanding the Asset Report ............................................................ 185
- Discovery Troubleshooting ...................................................................... 186
- Discovery Scheduling .............................................................................. 186

**Discovery Troubleshooting** ...................................................................... 189

- Collection Validation ............................................................................. 189
  - Credential Test .................................................................................. 189
  - Collection Validation ......................................................................... 190
  - Overall Status .................................................................................... 191
  - Result Codes ...................................................................................... 191
  - Failure Details .................................................................................... 193
  - Common Issues Resulting In A PARTIAL Status .................................. 194
  - Common Issues Resulting In An ERROR Status ................................ 195
- Protocol Specific Troubleshooting ............................................................. 195
- Discovery Help ....................................................................................... 196

### 4 Using the Platform ................................................................................. 199

**Building Application Stacks** ................................................................... 199

- Application Stacks Overview ................................................................. 199
- Part One: Build Application Stacks .......................................................... 200
- Part Two: Verifying Scope with RSG-Out of Scope Services .................... 201
- Part Three: Application Stack Review and Refinement ........................... 202
Foundation and CloudScape (formerly RISC Networks) helps you make better-informed decisions when moving your applications to the cloud. It provides complete, automated discovery of business applications, networks, security threats, dependency mapping and cloud migration planning, as well as business case analysis.

With Foundation and CloudScape, every IT decision will be well informed because you can illuminate your entire IT landscape. This insight empowers you to quickly and efficiently navigate to the cloud using an accurate analysis of what workloads should be migrated—and in what order.

To learn how to use Foundation and CloudScape, see the following sections:

| Table 1-1 • Foundation and CloudScape User Guide |
|-------------------------------------------------|------------------------------------------------|
| **Section**                                     | **Description**                                 |
| Foundation and CloudScape Overview              | Provides a technical introduction to the Foundation and CloudScape platform. You should understand what and how we collect, how we are architected and deployed, and our security procedures/policies. |
| Getting Started with Foundation and CloudScape | Explains how to deploy the virtual appliance, perform complete discovery with proper troubleshooting, and proceed to the performance collection phase successfully. |
| Using the Platform                              | Provides you with instructions on how to operate, interpret, and utilize the platform after the Discovery and Inventory phases are successfully completed. |
Product Support Resources

The following resources are available to assist you with using this product:

- Flexera Product Documentation
- Flexera Community
- Flexera Learning Center
- Flexera Support

**Flexera Product Documentation**

You can find documentation for all Flexera products on the Flexera Product Documentation site:

https://docs.flexera.com

**Flexera Community**

On the Flexera Community site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Flexera’s product solutions, you can access forums, blog posts, and knowledge base articles.

https://community.flexera.com

**Contacting Flexera Support**

For information on contacting Flexera Support via the Flexera Community, see the following topics:

- How to Register for Community Access
- Getting Started with Community
- Community Best Practices

**Flexera Learning Center**

Flexera offers a variety of training courses—both instructor-led and online—to help you understand how to quickly get the most out of your Flexera products. The Flexera Learning Center offers free, self-guided, online training classes. You can also choose to participate in structured classroom training delivered as public classes. You can find a complete list of both online content and public instructor-led training in the Learning Center.

https://learn.flexera.com

**Flexera Support**

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the Get Support menu of the Flexera Community.

https://community.flexera.com
Contact Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at:

http://www.flexera.com

You can also follow us on social media:

- Twitter
- Facebook
- LinkedIn
- YouTube
- Instagram
Foundation and CloudScape Overview

This section provides a technical introduction to the Foundation and CloudScape platform. You should understand what and how we collect, how we are architected and deployed, and our security procedures/policies.

- Architecture, Data Handling, and Security
- What We Collect
- How We Collect
- Deployment Requirements
- Alternate and Additional Deployment Methods

Architecture, Data Handling, and Security

For information about the architecture, data handling, and security of Foundation and CloudScape (formerly RISC Networks), see the following topics:

- Foundation and CloudScape Architecture
- RN150 Virtual Appliance Security
- Advanced Debugging
- Multifactor Authentication
Foundation and CloudScape Architecture

Data is collected by the RN150 at the client location and periodically exported, encrypted, and securely transmitted via TLS to the Secure Cloud Environment (SCE) which is the data repository for the engagement. The data is then accessed by browsing to portal.riscnetworks.com and logging in to the assessment portal.

Secure Cloud Deployment

Figure 2-1: Foundation and CloudScape Networks Architecture

RN150 Virtual Appliance Security

Information about RN150 virtual appliance security is described in the following sections:

- Advanced Operating System
- Encrypted Credentials
- Data Handling and Storage

Advanced Operating System

The virtual appliance is based on the Debian/GNU Linux 10 operating system. No access to the appliance is allowed with any protocol with the exception of a RISC Networks management session and those connections initiated by the appliance itself. SSH and ICMP are allowed but are used solely for connectivity testing and troubleshooting. Technology built into
RISC Networks’ system allows for a stateful operating system on the virtual appliance for the duration of the assessment. For this reason it is recommended that the virtual appliance be deleted at the successful completion of an assessment following the customer’s process for data handling and deletion.

**Encrypted Credentials**

Customer security and the proper handling of network credentials are of the utmost importance to RISC Networks as well our partners and customers. To guarantee this security, RISC Networks has implemented the following features with regards to handling credentials:

- Credentials are encrypted via AES-256 immediately upon being entered through the appliance web interface.
- Credentials remain encrypted on the appliance for the duration of the assessment and will be deleted at the time the appliance image is deleted from memory.
- Credentials are NEVER uploaded to RISC Networks’ SCE.
- RISC Networks delivery engineers never know or have access to the credentials used to bootstrap the appliance.

**Data Handling and Storage**

All data is uploaded from the virtual appliance to the RISC Networks SCE using 256-bit TLSv1.2 encryption (AES-256). Before being uploaded, the raw data is encrypted at rest using AES-256 with a 2048-bit asymmetric public key (RSA-2048). Data uploads will occur on regular intervals in order to limit the upload size and are encrypted at rest in a secure repository that is not directly accessible from the Internet.

The encrypted raw data is accessed by the Foundation and CloudScape platform and is decrypted, stored in transient database instances and accessed for report generation. Final reports are placed into storage and accessible only through the RISC Networks secure web portal for download by customers and partners.

Raw customer assessment data is held in RISC Networks’ SCE for a period of up to 35 days past the subscription end date. After the subscription expires, the data is deleted and the storage device that data was stored on returns to the pool of data storage available for other RISC Networks’ engagements. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to ensure customer data are not exposed to unauthorized individuals. RISC Networks storage device are decommissioned using the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures the device will be degaussed or physically destroyed in accordance with industry-standard practices.

**HealthCheck**

For customers utilizing our HealthCheck product, raw customer data is held in RISC Networks SCE for a period of 90 days after the assessment has ended. After 90 days, the data is deleted and the storage device that data was stored on returns to the pool of data storage available for other RISC Networks engagements. When a storage device has reached the end of its useful life, procedures include a decommissioning process that is designed to ensure customer data are not exposed to unauthorized individuals. RISC Networks storage device are decommissioned using the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures the device will be degaussed or physically destroyed in accordance with industry-standard practices.
Data Confidentiality and Compliance

Privacy and security of Customer’s information, including personal data, are a primary concern for RISC Networks. RISC Networks’ data centers adhere to strict regulatory compliance standards such as:

- PCI DSS Level 1
- SAS 70
- ISO 27001

At the end of any engagement, RISC Networks anonymizes data for aggregation reporting.

RISC Networks does not collect personal user data such as:

- User logins or passwords
- Data Files (office documents, text files, etc)
- Email Files
- Database Files
- Any files containing user information
- Application payload information

To the extent that any particular engagement requires the processing of personal data in the EU and their subsequent transfer outside of the EU, RISC Networks, will, as a data processor, upon request, enter into the EU Standard Contractual Clauses for the transfer of personal data to third countries. In addition, RISC Networks is classified as a “Data Processor” under EU privacy laws and shall act only on instructions from its Customer and will have adequate technical and organizational security measures in relation to the processing of any personal data.

Advanced Debugging

RISC Network’s understands and respects the data privacy concerns of our customers. Under certain support circumstances it may be necessary for RISC Networks’ engineers to access a deployed appliance for advanced troubleshooting and support scenarios. This option is not enabled by default.

In order to exercise this option, we require the customer to enable the Advanced Debugging option on the appliance itself. Advanced Debugging and troubleshooting allows shell commands to be executed and reviewed remotely from the RN150 or FlexDeploy appliances by select RISC Networks’ Senior Developers and Engineers. This allows us to review log files, running process and the overall status of the appliance for troubleshooting and support purposes.

- Only select RISC Networks' Senior Developers and Engineers have the ability to assist in this manner.
- Troubleshooting and analysis could include a review of discovery results and inventory data from the appliance.
- No data is stored off site but is reviewed within a temporary session. The communication is facilitated through an outbound SSL encrypted session from the FDP or RN150 to riscnetworks.com(no inbound connectivity is required).

Advanced Debugging can be enabled (or disabled) from the Dashboard of the RN150 and from the Interface configuration screen of the FlexDeploy. The Flexera Support will provide specific instructions, based on the appliance type and version, in the event Advanced Debugging is requested.
Multifactor Authentication

Multifactor Authentication (MFA) is now available in order to provide an additional layer of security for our users. With MFA, logging in to the platform requires an additional step: providing a six-digit token texted to your cellphone or a secondary email address. Subsequent logins to the Foundation and CloudScape platform from the same device will allow you to bypass the MFA portion of login until either 30 days has passed or you log in from another device. When logging in from a different device, you'll be asked to re-authenticate with MFA.

Task  To register for multifactor authentication:

1. Log into the Foundation and CloudScape platform. The following screen opens, prompting you to enter multi-factor authentication preferences.

2. Enter both a cell phone number and a secondary email address, and select either one as a default. The information you enter should be where you wish to receive tokens for multi-factor authentication from Flexera.

3. Click Save Preferences. The following screen opens, prompting you to check your email for an activation code.
Note • This screen also includes a Click here link that you use to make changes to your multi-factor authentication preferences that you just specified on the previous screen.

4. Navigate to your email (the email used for login). You should receive an email from noreply@riscnetworks.com that looks like the one below:

Confirm Your MFA Registration For RISC Networks

noreply@riscnetworks.com
Today, 9:21 AM

You have registered the following devices for MFA with RISC Networks:

- Cellphone: 9684
- Email: abc@abccompany.com
- Default Device: cellphone

Please click here to finalize your registration.

5. If the preferences match what you entered in the portal and wish to register, click the click here link (or copy the link and paste it in your browser). You will be redirected back to the portal, and after a moment, the following screen will open:
At this point, a token will have been sent to your default device.

- If you do not have access to the default device (such as if you lost your cellphone), you may select the alternative option from the drop-down list and click Resend to deliver to token to the alternative address.
- Similarly, if you did not receive the token, you can click Resend to redeliver it.

*Note* • *Email tokens can take a few minutes to arrive, while cellphone tokens are typically delivered in a matter of seconds. Please check spam/junk folders if the email doesn’t arrive shortly.*

6. Enter the token that was delivered to your device into the **Authentication Code** box and click **Login** to authenticate the token.

- If you entered a valid token, you will be directed to the Assessment Selection screen.
- If you entered an invalid token, you can re-enter and try again or resend a new token and authenticate with it.

### What We Collect

The following list outlines the specific information sets gathered by the RISC Networks RN150 collecting appliance during an engagement. Data is collected in two distinct phases by the RN150, inventory and performance.

- Network Equipment
- Windows Servers
- Linux/Unix Servers
- VMware
- Databases

*Note* • *For documentation on access requirements please see How We Collect.*
# Network Equipment

For network equipment, the following information is collected:

**Table 2-1 • Information Collected for Network Equipment**

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Hardware</td>
<td>• Serial Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Line Cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flash Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Memory Size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interface Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ENTITY-MIB information</td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>• Software version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Flash file list</td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td>• Routing Table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ARP Table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• L2 Forwarding Table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Neighbor Information (CDP, FDP, LLDP, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Spanning Tree Topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SAN Switch Forwarding Information (WWN Names, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SCSI Lun Information (FC Switches only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quality of Service Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco IP SLA Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Netflow Configuration</td>
</tr>
<tr>
<td>Performance</td>
<td>Statistical</td>
<td>• Interface Utilization and Error Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPU and Memory Utilization Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco MQC Statistics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP SLA Statistics (TrafficSim)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Netflow flow information (TrafficWatch)</td>
</tr>
</tbody>
</table>
## Windows Servers

For Windows Servers, the following information is collected:

### Table 2-2 • Information Collected for Windows Servers

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Hardware</td>
<td>• Serial Number (Dell Service Tag, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical Hard Drive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HBA Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Card information</td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>• OS Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Installed Applications and versions with process ID information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Services and status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Logical Disks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Shares</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTP get on port 80</td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td>• Windows Event Log information (3 days of Errors and Warnings)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Citrix Metaframe Server Inventory</td>
</tr>
<tr>
<td>Performance</td>
<td>Statistical</td>
<td>• CPU Performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Process specific Performance metrics (CPU, Swap, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Memory Performance (bytes used / % used )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disk (Logical and Physical) performance (I/O per sec, I/O bytes, latency, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Network Interface Utilization (I/O bytes, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Process Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Netstat Connectivity Information (opt-in only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DNS A records and C names where applicable</td>
</tr>
</tbody>
</table>
Linux/Unix Servers

For Linux/Unix Servers, the following information is collected:

Table 2-3 • Information Collected for Linux/Unix Servers

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory via SNMP and SSH</td>
<td>Hardware</td>
<td>• Physical Memory&lt;br&gt;• Physical CPU&lt;br&gt;• Physical Hard Drive&lt;br&gt;• Network Interfaces</td>
</tr>
<tr>
<td></td>
<td>Software</td>
<td>• OS Description&lt;br&gt;• Installed Applications and versions with process ID information&lt;br&gt;• Logical Disks&lt;br&gt;• Filesystems&lt;br&gt;• HTTP get on port 80</td>
</tr>
<tr>
<td>Inventory via SSH</td>
<td>Software</td>
<td>• Operating System&lt;br&gt;• OS Version&lt;br&gt;• OS Distribution&lt;br&gt;• OS Distribution Version&lt;br&gt;• CPU Architecture</td>
</tr>
<tr>
<td>Performance via SNMP and SSH</td>
<td>Statistical</td>
<td>• CPU Performance&lt;br&gt;• Memory Performance (bytes used / % used)&lt;br&gt;• Physical Disk I/O&lt;br&gt;• Running Processes&lt;br&gt;• Socket Connectivity Information (uses TCP-MIB via SNMP / prefers RFC 4022 version)&lt;br&gt;• Network Interface Utilization</td>
</tr>
</tbody>
</table>
**VMware**

For VMware Servers, the following information is collected:

**Table 2-4 • Information Collected for VMware Servers**

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Hardware</td>
<td>• Server Model</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disk Information (size and configuration)</td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>• Guest Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OS Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ESX Location</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Host Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OS Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DataStore mapping to hosts and guests</td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td>• Virtual Switch configuration</td>
</tr>
<tr>
<td>Performance</td>
<td>Statistical</td>
<td>• CPU Utilization (wait time, ready time, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Memory Utilization (usage MB, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disk Utilization (I/O / sec, bytes/sec, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Utilization (bytes in/out)</td>
</tr>
</tbody>
</table>

**Databases**

For databases, the following information is collected:

**Table 2-5 • Information Collected for Databases**

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Database</td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Schemas Names (sometimes referred to as database names)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Table Metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Table Names</td>
</tr>
</tbody>
</table>
Table 2-5 • Information Collected for Databases (cont.)

<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>Information Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>Statistical</td>
<td>• Connectivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Table Names</td>
</tr>
</tbody>
</table>

How We Collect

This section outlines the process the RISC Networks RN150 virtual appliance follows once a customer has deployed the appliance and begun the first scan.

The RN150 collects data in three distinct stages: Discovery, Inventory, and Performance. The details of each of these stages are below.

![Collection Process for Virtual Appliances](image)

Figure 2-2: Collection Process for Virtual Appliances
The details on the collection process are listed in the following table:

**Table 2-6 • Collection Process for Virtual Appliance Details**

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discovery Stage</strong></td>
<td>The virtual appliance performs network discovery using standard network mapping software. The virtual appliance will only scan the subnets that are provided into the RN150 virtual appliance by the Customer and/or Partner. This stage of the Analytics engagement is designed to introduce minimal amounts of traffic onto the network and is therefore rate limited. A class B subnet typically takes about 2.5 hours to scan. During this stage, the appliance will perform an ICMP sweep on the input subnets and then will perform a select port scan on those IPs that respond to ping. If a device is found to have an open port corresponding to one of our credential types we will then attempt to access the device given the provided credentials. The RN150 will cycle through relevant credentials until it makes a successful match or fails entirely. All devices that respond to ping and are successfully accessed via the credentials are considering “Interesting Devices.” This ends the discovery stage.</td>
</tr>
<tr>
<td><strong>Inventory Stage</strong></td>
<td>During this stage the appliance revisits those “Interesting Devices” determined during the Discovery Stage using the matched credentials to gather workload specific data. All workload specific data is then compressed, encrypted, and uploaded via a secure SSL connection to the RISC Networks’ SCE. At the end of the inventory phase a populated asset report and licensing page will be available in the RISC Networks portal. The user can then select devices within the licensing page that will move on to the Performance Stage. This ends the Inventory Stage.</td>
</tr>
<tr>
<td><strong>Performance Phase</strong></td>
<td>Once devices have been licensed within the portal performance collection occurs via any matched credential type. Performance statistics are accessed at an interval of no greater than 1 sampling every 5 minute interval. During this stage the RN150 virtual appliance sends regular uploads to the RISC Networks’ SCE for processing and access within the portal. The upload frequency and size is determined algorithmically to limit impact on the host network. The performance stage continues as long as the partner/customer has an active subscription and has devices licensed.</td>
</tr>
</tbody>
</table>

*Note* • *For information on what data is collected at each stage, see What We Collect.*
**Collection Specifics**

More detailed technical descriptions of some of our collection methods can be found in the following sections:

- Windows Collection Module
- SSH Collection Module
- Database Module
- Load Balancers
- AWS Collection Module
- Performance Counter Disambiguation
- ServiceNow Configuration and User Guide
- Configuration Items in ServiceNow

**Windows Collection Module**

The Windows Collection Module provides data collection for Windows server and workstation systems as part of the RISC Networks engagement process. It uses the Windows Management Instrumentation (WMI) and Server Message Block (SMB) protocols to communicate with in-scope discovered devices to collect identifying inventory data as well as ongoing performance data.

- WMI
- Remote Commands
- Windows Collection Module Troubleshooting
- Windows Collection Module References

**WMI**

WMI is a standard component of the Microsoft Windows operating system since its introduction in Windows 2000. See the References section for links to Microsoft documentation on WMI. The Windows Collection Module uses the standard wmic utility to issue read-only WMI Query Language (WQL) queries to the WMI service on Windows devices.

The following WMI providers are queried:

**Table 2-7 • WMI Providers**

<table>
<thead>
<tr>
<th>WMI Provider Class</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win32_ComputerSystem</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_OperatingSystem</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_ComputerSystemProduct</td>
<td>No</td>
</tr>
<tr>
<td>Win32_Bios</td>
<td>No</td>
</tr>
<tr>
<td>WMI Provider Class</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Win32_SystemEnclosure</td>
<td>No</td>
</tr>
<tr>
<td>Win32_Process</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_DiskDrive</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_Volume</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_LogicalDisk</td>
<td>No</td>
</tr>
<tr>
<td>Win32_Share</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_NetworkAdapter</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_NetworkAdapterConfiguration</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_Service</td>
<td>No</td>
</tr>
<tr>
<td>Win32_Process</td>
<td>Yes</td>
</tr>
<tr>
<td>MSFC_FCAdapterHBAAttributes</td>
<td>No</td>
</tr>
<tr>
<td>MSFC_FibrePortHBAAttributes</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfRawData_PerfOS_Process</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_PerfRawData_PerfDisk_LogicalDisk</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_PerfRawData_PerfDisk_PhysicalDisk</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_PerfRawData_PerfProc_Process</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfRawData_Tcpip_NetworkInterface</td>
<td>Yes</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_TermService_TerminalServices</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_TermService_TerminalServicesSession</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_IMAService_CitrixIMANetworking</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_CitrixLicensing_CitrixLicensing</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_MetaFrameXP_CitrixMetaFramePresentationServer</td>
<td>No</td>
</tr>
<tr>
<td>Win32_PerfFormattedData_CitrixICA_ICASession</td>
<td>No</td>
</tr>
<tr>
<td>Win32_NTEventlogFile</td>
<td>No</td>
</tr>
</tbody>
</table>
Remote Commands

Some data collected by the Windows Collection Module is not available through WMI. For this data, the Windows Collection Module uses a facility for running commands on Windows hosts through \texttt{cmd.exe}. The \texttt{wmiexec.py} utility from the open source Impacket project is used to provide this facility.

The process uses the SMB and WMI protocols. First, a WMI session is established with the remote Windows system, and an SMB session is established with the \texttt{ADMIN$} share. The WMI \texttt{Win32\_Process} provider is used to invoke a new process through the \texttt{cmd.exe} command interpreter. The output of the command that is invoked is redirected to a file in the \texttt{ADMIN$} share, and the contents of this file is read using the established SMB connection. Once all of the data has been read from the output file, the file is removed and the SMB and WMI sessions are torn down.

The output file created during this process uses an established naming convention. The name begins with two underscore characters. This is followed by the current epoch time (the number of seconds that have elapsed since January 1st, 1970), a period, and two fractional second digits. For example, \texttt{__1497992728.46}.

The final form of the command as invoked on the remote Windows service, where \texttt{COMMAND} is replaced by the command requested by the Windows Collection Module and \texttt{FILENAME} is replaced by a filename in the format described above:

\begin{verbatim}
cmd.exe /Q /c COMMAND 1> \127.0.0.1\ADMIN$\FILENAME 2>&1
\end{verbatim}

Remote commands support encrypted SMB sessions if the SMB server is configured for encryption. Versions 3, 2, and 1 of the SMB protocol are supported, and the session will use the highest protocol version advertised by the server.

For more information about remote commands, see the following sections:

- Remote Command Reference
- Netstat
- Installed Applications Registry Query
- Local DNS Cache
- CHCP
- Configuration File Collection

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{WMI Provider Class} & \textbf{Required} \\
\hline
Win32\_NTLogEvent & No \\
\hline
MicrosoftDNS\_AType & No \\
\hline
MicrosoftDNS\_CNAMEType & No \\
\hline
\end{tabular}
\caption{WMI Providers}
\end{table}
Remote Command Reference

The following table list remote commands.

Table 2-8 • Remote Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>netstat -anop TCP</td>
<td>Reports network connections.</td>
</tr>
<tr>
<td>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /s</td>
<td>Reports installed applications.</td>
</tr>
<tr>
<td>reg query HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall /s</td>
<td>Reports installed 32-bit applications on a 64-bit host.</td>
</tr>
<tr>
<td>ipconfig /displaydns</td>
<td>Reports cached DNS name lookups.</td>
</tr>
<tr>
<td>chcp.com</td>
<td>Reports the console code page, used to determine text encoding format.</td>
</tr>
<tr>
<td>powershell Get-Content -Path PATH</td>
<td>Retrieves the content of the file at path PATH (see Configuration File Collection).</td>
</tr>
</tbody>
</table>

Netstat

The netstat command shown above reports the network connections currently active on the remote Windows host. This is used as a critical component in grouping Application Stacks and reporting application dependencies in the environment. This command is executed during the Performance collection process.

The formulation of the command is as follows:

Table 2-9 • Netstat Command Formulation

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Displays all connections and listening ports</td>
</tr>
<tr>
<td>-n</td>
<td>Displays connections numerically, rather than resolving them to hostnames or service names</td>
</tr>
<tr>
<td>-o</td>
<td>Displays the process ID (PID) that has bound the socket</td>
</tr>
<tr>
<td>-p</td>
<td>TCP filters the results to the TCP protocol only</td>
</tr>
</tbody>
</table>

Installed Applications Registry Query

The reg query command shown above queries the Windows Registry for information regarding installed software. This is a read-only query. The response data includes a number of key-value pairs describing the installed software, which is filtered down to a subset of keys. This data is used for a variety of purposes, including the Application Matching and Security Module features. This command is executed during the Inventory and Performance collection processes.
Local DNS Cache

The `ipconfig /displaydns` command shown above is used to collect the contents of the local DNS cache from a Windows system, the DNS names that the system has recently requested. This feature is enabled by default, but may be disabled by accessing the Appliance Settings section within the Assessment page on the RN150 appliance and toggling the Windows DNS Cache Collection feature to the Off position.

CHCP

To better support international customers, the RN150 appliance will automatically run the `chcp.com` command when first interacting with a Windows system. This allows the RN150 to determine what text encoding is used by that system when interpreting the results of a remote command. The RN150 will only run this command once for a given system and will store the results for future use; however if the RN150 is not able to execute this command, or if data collection is not successful for that system, the command may be run on future attempts to communicate with that system.

Configuration File Collection

The RN150 supports an optional feature, disabled by default, that collects the content of configuration files installed on the system. For Windows devices, this includes IIS configuration files. If the feature is enabled and IIS application services are determined to be running on a Windows device, the content of the following directory is retrieved, along with any app pool configuration files listed as an argument to the running IIS process or loaded from the `applicationHost.config` file:

```
C:\Windows\System32\inetsrv\config\applicationHost.config
```

Windows Collection Module Troubleshooting

For Windows devices we get error messages (NT STATUS codes) to assist in troubleshooting. Those common error messages are listed below:

**Table 2-10 • NT Status Codes**

<table>
<thead>
<tr>
<th>Error</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTSTATUS: NT_STATUS_CONNECTION_REFUSED - NT_STATUS_CONNECTION_REFUSED</td>
<td>Non-Windows device, Firewall rule – verify the IP address is a Windows device and there are no access restrictions between the virtual appliance and the end device</td>
</tr>
<tr>
<td>NTSTATUS: NT_STATUS_ACCESS_DENIED - Access denied</td>
<td>Invalid username/password, user account is not Domain Administrator or Local Administrator – verify username/password is correct, verify username is either domain administrator or local administrator account</td>
</tr>
<tr>
<td>NTSTATUS: NT_STATUS_IO_TIMEOUT - NT_STATUS_IO_TIMEOUT</td>
<td>Firewall, host unreachable – verify there are no access restrictions between the virtual appliance and the end device</td>
</tr>
<tr>
<td>NTSTATUS: NT_STATUS_HOST_UNREACHABLE - NT_STATUS_HOST_UNREACHABLE</td>
<td>The remote network is not reachable by the transport – verify host is IP reachable</td>
</tr>
<tr>
<td>NTSTATUS: NT_STATUS_NETWORK_UNREACHABLE - NT_STATUS_NETWORK_UNREACHABLE</td>
<td>The remote network is not reachable by the transport – verify host is IP reachable</td>
</tr>
</tbody>
</table>
Windows Collection Module References

For additional information on the Windows Collection Module, see the following sites:

- Windows Management Instrumentation
- Windows Management Instrumentation: Background and Overview
- What is Impacket?

SSH Collection Module

The SSH Collection Module provides data collection for Linux and UNIX-class systems as part of the RISC Networks engagement process. It uses the Secure Shell (SSH) protocol to communicate with in-scope discovered devices to collect identifying inventory data as well as ongoing performance data.

SSH is an industry-standard protocol that provides an encrypted, authenticated channel of communication between devices, forming the backbone of most systems’ orchestration frameworks today. The SSH Collection Module acts as an SSH client to communicate with SSH servers running on devices in the environment. The SSH Collection Module utilizes OpenSSH, the current de-facto standard SSH distribution.

Previously, collection from Linux and UNIX-class systems was conducted using the SNMP protocol. While SNMP is still supported for these device types, the SSH Collection Module can replace the SNMP protocol for all data collection. The SSH Collection Module does not support collection from network devices, which still require the use of SNMP. Details on system eligibility for participation in the SSH Collection Module are provided below.

Note • Please note that the SSH Collection Module is a separate feature from the CLI data collection process for Cisco network devices using the telnet/SSH protocols.

For more information on the SSH Collection Module, see the following topics:

- SSH Collection Module Overview
- Supported Operating Systems
- System Eligibility
- Credential Utilization
- User Account Requirements
- Authentication Types
- Key-Based Authentication Requirements
- Privilege Elevation
- Entering Credentials
- Custom Server Ports
- Configuration Examples
- SSH Collection Module Command Reference
- SSH Collection Module Troubleshooting
Chapter 2  Foundation and CloudScape Overview

How We Collect

SSH Collection Module Overview

When the SSH credentials section has been opted-in on the RN150 Virtual Appliance, and at least one SSH credential has been entered, the SSH Collection Module will be utilized to attempt to collect data from discovered devices that meet the eligibility requirements.

The RN150 Virtual Appliance acts as an SSH client that will connect to devices, authenticate using the provided credentials, issue commands on the remote system, and collect the output of those commands. The commands that are issued using the SSH Collection Module are documented below.

Supported Operating Systems

The SSH Collection Module does not currently support all UNIX-class operating systems, although additional systems will be released over time. The currently supported systems are:

- Linux
- IBM AIX

For Linux, the SSH Collection Module is not distribution-specific, but due to the wide variety of distributions and subtle differences between them, it may be the case that niche or very old distributions are not accounted for by the SSH Collection Module. In this case, a support case can be opened for evaluation, and/or SNMP can be used to collect from these systems. At the time of this writing, the following Linux distributions are considered fully supported by the SSH Collection Module:

- RHEL/Oracle/CentOS 5.x, 6.x, 7.x
- Ubuntu 12.04, 14.04, 16.04
- SUSE Linux Enterprise Server 9, 10, 11, 12
- IBM AIX

System Eligibility

For a system to be considered eligible for participation in the SSH Collection Module, a set of conditions must be met. Some of these conditions are common to all protocol types used in the engagement process, and some are specific to the SSH Collection Module:

Common Requirements

- The system responds to an ICMP Echo Request (ping) sourced from the RN150 Virtual Appliance
- The RN150 Virtual Appliance can communicate over TCP or UDP to the system
- The protocol type has been opted-in to on the RN150 Virtual Appliance
- At least one credential for the protocol has been entered in the RN150 Virtual Appliance

SSH Collection Module Requirements

- The system has a running SSH server
- The RN150 Virtual Appliance is permitted to communicate with the system via the server TCP port
The system firewall permits communication to the server TCP port from the RN150 Virtual Appliance IP

- The SSH server is configured to allow connections from the RN150 Virtual Appliance
- The SSH server is configured to allow the authentication type selected for the provided credential
- The user account associated with the credential is a valid account on the system
- The user account has a valid shell
- The user account is permitted to utilize sudo, unless using the root account
- sudo is configured according to the requirements listed below
- The operating system is understood and supported by the SSH Collection Module

**Credential Utilization**

The SSH Collection Module utilizes a process common with other protocol types such as SNMP and WMI. When a system is discovered, meaning it responds to an ICMP ping and is found to have TCP port 22 available (or an alternate port, see section Custom Server Ports below), the SSH Collection Module will iteratively utilize each provided SSH credential to attempt to authenticate with the system. The first credential that is successful in connecting and authenticating, and for which other validation checks are successful, will be mapped to that device. Further communication with the system will be conducted using that particular credential entry.

This allows the user to enter a single credential that will be valid for use by any systems that are configured to utilize that credential, and the user will only need to enter each unique credential that is intended to be utilized. As the SSH Collection Module does not know at the outset which credential entry maps to which device(s), this may result in a number of failed authentication attempts as the SSH Collection Module tries each credential to derive the correct entry for a given system. An IPS or other system that monitors failed authentication attempts may be triggered by this behavior. In this case, an exception may need to be made for the purposes of the SSH Collection Module.

**User Account Requirements**

The SSH protocol authentication process centers around a user account. All forms of authentication will require a username. The username requirements of the SSH Collection Module module are the requirements of the SSH protocol, including but not limited to:

- The user account must be a valid, known user account on the target system
- The user account must be enabled
- The user account must have a valid shell permitting login
- The user account must be permitted to perform login via SSH

Some systems will not include the /sbin directory in the default command $PATH. For reference, the environment variable $PATH contains a colon-delimited list of directories that the shell searches for commands that are not provided using absolute paths. Some commands required by the SSH Collection Module are located in the /sbin directory, and if this is not included in the $PATH, attempts to utilize the commands will fail. It is highly recommended that the /sbin directory be included in the $PATH for the user account being utilized. Details on this are shown in the configuration examples below.
Authentication Types

The SSH protocol provides a number of different authentication mechanisms for providing alternative data, beyond the username, for authenticating with the SSH server. The following authentication mechanisms, described using the SSH terminology, are supported by the SSH Collection Module:

- password
- keyboard-interactive
- publickey

The password and keyboard-interactive authentication types are both password based. The password type performs a direct user password validation facility, while the keyboard-interactive type uses the PAM infrastructure. Configuration on the RN150 Virtual Appliance for either type is identical, and the password string should be provided as a component of the credential entry.

The publickey authentication type uses asymmetric key pairs, most often RSA keys. In this model, the private key of the pair is utilized by the client, while the corresponding public key is attached to the user account on the server. As the SSH Collection Module on the RN150 Virtual Appliance is acting as the client, the private key of the pair is provided as a component of the credential entry, while the public key is a component of the user account configuration on the target systems. More details on enabling publickey authentication is provided below.

Key-Based Authentication Requirements

There are a variety of differing key types supported by various SSH implementations. As the SSH Collection Module uses the OpenSSH distribution for the SSH client, the key type used must be understood by OpenSSH.

The requirements for keys provided as part of an SSH credential entry for the SSH Collection Module are as follows:

- The private key must be in the ASCII PEM encoding, which is the default when generated using the ssh-keygen utility

Certain key generators, will generate a binary-form key file. If such a key is desired to be used, it must first be converted to ASCII PEM format prior to use. Consult the documentation for the key generator software for details on key conversions. It is highly recommended that the conversion is performed on a copy of the key, and that the successful utilization of the key is validated prior to use as a credential entry for the SSH Collection Module.

Private keys generated by the PuTTY client popular on Windows platforms are not directly compatible with the OpenSSH client, although the OpenSSH server supports validation of PuTTY public keys. These keys will need to be converted to the OpenSSH format prior to use.

Privilege Elevation

Some commands utilized during the collection processes require elevated privilege on the target system. This corresponds to elevation to the root account. The specific commands requiring elevated privilege are provided below.

If the username associated with the credential entry is exactly root, then no additional privilege elevation will be attempted when issuing commands. Any other username involves the use of the sudo utility to perform the elevation. The sudo utility is ubiquitous in the Linux and UNIX-class system space, and will be provided by the operating system for many systems and/or distributions.

The use of sudo introduces several requirements for configuration, and is typically the most involved portion of configuring the environment for participation in the SSH Collection Module.
sudo is typically password-based, and was designed for interactive use. Particularly, an interactive session on a system will involve a terminal device, or TTY, that is associated with the login shell of the session. When using the SSH protocol as a communication transport in a non-interactive manner, a TTY device on the target system is not allocated. Due to the automated nature of the SSH Collection Module, this means that the SSH Collection Module will not allocate a TTY.

In order to provide sudo with a password, the utility typically requires a TTY device to present a password entry prompt. As the SSH Collection Module does not allocate a TTY, this facility is not currently supported. In order to configure sudo to participate in the SSH Collection Module, the requirement of an associated TTY device must be disabled, and sudo must be configured to not prompt for a password. Both of these configuration items can be set on a per-user basis, either on the existing user account associated with the credential entry, or as a component of a specific account created for the purposes of utilizing the SSH Collection Module as part of the RISC Networks engagement process. Details on how to configure sudo for these requirements are provided below.

Entering Credentials

In order to participate in the SSH Collection Module, SSH authentication credentials must be provided to the SSH Collection Module via the RN150 Virtual Appliance credential configuration dialog. As stated above, you will only need to enter each unique credential that is intended to be used, which will be utilized for each system for which that credential is found to be successful.

To enter an SSH credential in the RN150 Virtual Appliance, access the configuration application on the appliance by using the virtual console or by browsing to the appliance IP address via HTTP or HTTPS. From the Dashboard page of the application, select the SSH section. Please note that the SSH Collection Module and the Cisco CLI collection module are different technologies, and to utilize the latter you will need to access the Additional Credentials section, select CLI, and provide credentials there.

Accessing the SSH section will provide an input form for entering credential entries. The exact process of entering a credential varies slightly depending on the authentication type being used for that particular credential entry.

For all authentication types, first enter the username for the credential in the Username field.

Next, from the drop-down list entitled Auth Type, select the type of authentication desired. This will currently be one of password or publickey. The password type should be selected for either password or keyboard-interactive authentication.

If password is selected, an additional entry field will be presented, in which the password should be entered.

If publickey is selected, two input fields will be presented. The full text contents of the private key associated with the credential should be pasted in the Private Key text field. Please note that if the virtual console does not permit copy-and-paste, it may be necessary to access the appliance configuration application over HTTP or HTTPS in order to paste in the contents. The key contents must be PEM encoded ASCII text. The key contents will typically begin and end with a header field, which should be included in the entered text. If the private key being used in the credential entry is passphrase-encrypted, the passphrase associated with the key should be entered in the Key Passphrase field. If the key requires a passphrase and one is not provided, that key will not be able to be successfully used by the SSH Collection Module. If the private key is not passphrase-encrypted, then the Key Passphrase field should be left blank. If a passphrase is entered for an unencrypted key, this will not prevent the SSH Collection Module from successfully using the key, but may be confusing later on or to other users participating in credential entry. If a passphrase-encrypted key is entered without a passphrase and committed to the credentials list, editing that entry will allow the addition of a passphrase.

The Privilege Elevation field is currently not able to be explicitly set by the user, and the value of this field will be automatically determined based on the username provided. If the username is exactly ‘root’, then the value will be set to None, while any other username will cause the value to be set to sudo.
The Port field specifies the TCP port the client should connect to when utilizing the credential. Port 22 is the default, and will be automatically populated in the field. Any valid TCP port, with some exceptions, can be entered instead. See the Custom Server Ports section for more information.

Once the credential entry form is completed, select the Add button. This will present a further dialog, similar to other credential types. This dialog will present a text form that will be auto-populated with the IP address of the default gateway of the RN150 Virtual Appliance network interface. You can replace this IP address with the IP address of a known system that meets the eligibility requirements to test the operation of the credential to that system. It is highly recommended to test each credential that is entered, and if the credential is valid for a number of systems, it is further recommended to test to a sample of these systems. If the Test button is selected, the credential will be attempted against the provided IP address, and if successful, the credential will be added to the list of provided credentials. If the attempt is unsuccessful, the response from the target system will be shown in the dialog where you can either select a different IP address to test or select Cancel to alter the configuration of the credential. If the test is not desired, then Skip can be selected to immediately add the credential.

The SSH credential page will display some information about the credentials that have been entered. If an existing credential needs to be modified, then select Edit to open a configuration dialog where the values can be manipulated. Please note that manipulating an existing entry will change the credential for all systems in inventory that are mapped to the credential, and can result in a loss of communication with those system using the SSH Collection Module. If an existing credential needs to be tested to another known system, then you can select Edit, then without modifying the credential select Update. This will bring up the testing dialog described earlier.

If a credential needs to be deleted, then select the Delete button. Please note that deleting a credential will render it unusable for any systems that have been mapped to that credential, and can result in a loss of communication to those systems using the SSH Collection Module.

**Custom Server Ports**

The SSH Collection Module allows you to set an alternate TCP port for a given credential entry. The SSH protocol uses TCP port 22 as a standard, however some environments may run SSH servers on alternate ports. The TCP port selected when entering a credential is localized to that specific credential entry. Be aware, however, that when an alternate port is provided as a component of an SSH credential entry, that TCP port will be included in the discovery process, and that port will be checked for every IP address that responds during the ICMP portion of discovery to determine if that IP address supports SSH. If a device is found to have that TCP port open, then the device will be considered to support SSH.

Custom SSH ports provided for SSH credentials must meet a set of criteria to be accepted as a valid credential. To meet these criteria, a port must be numeric, within the range of valid TCP ports (1 - 65535), and not conflict with the standard ports utilized by other collection protocols. The following ports, and their related protocols, are not considered valid SSH ports: 80 (HTTP), 443 (HTTPS), 135 (WMI), 161 (SNMP), 62078 (iphone-sync).

Because user-supplied port numbers are automatically added to the list of ports used during the discovery process, a limitation on the number of unique custom ports is enforced. The credential configuration interface will produce an error indicating this limit if it is reached. The limit reflects the count of unique port numbers across all credential entries, not the number of credential entries using custom ports. When modifying the port on an existing credential, the new port number must also satisfy the custom port count limitation.

If a credential entry with a custom SSH port is removed, and the associated port number is not present on another credential entry that has not been removed, then the port will not be included in the discovery process and will not count towards the custom port count limitation.
Configuration Examples

Important • The configuration examples shown here are for informational and illustrative purposes only, and are not indented to be used directly. Always consult the documentation for your systems and fully understand the ramifications of configuration changes prior to implementation.

The following are some specific examples of how a system may be configured to participate fully in the SSH Collection Module. Your mileage with these examples will vary depending on the specifics of the system, the configuration requirements for the system or the environment, and other factors. All examples below assume that the user account being utilized is named ‘risc’, and the IP address of the RN150 Virtual Appliance is 10.0.0.2. The examples are provided in a pseudo-shell format, where lines prefixed with the ‘#’ symbol represent comments about the operation being performed while those that do not begin with ‘#’ are shell-like commands.

• Creating a User Account On Linux
• Creating A Key Pair
• Testing Sudo Configuration
• Basic Example Sudo Configuration
• Advanced Example Sudo Configuration

Creating a User Account On Linux

This is an example of how to create a user account on a Linux system.

Note • This is for illustrative purposes only. Consult the Linux documentation for your system before attempting to create a user account.

Task To create a user account on Linux:

1. Create the user account.
   
   useradd -m risc

2. Set the user’s password.
   
   passwd risc

3. Configure the PATH and LC_ALL variables for the user account by modifying the shell initialization files.
   
   echo 'export PATH=${PATH}/sbin' >> ~/.bashrc
   echo 'export LC_ALL=C' >> ~/.bashrc
Creating A Key Pair

This is an example of how to create an SSH key pair. The example assumes that the user account used for collection is named 'risc'.

Task | To create a key pair:
--- | ---
1. Log in to the account.
   ```bash
   su - risc
   ```
2. Create a keypair. This example uses the default configuration. See the ssh-keygen manual for configuration options.
   ```bash
   ssh-keygen
   ```
3. Add the public key to the list of keys allowing login to the local system.
   ```bash
   cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
   ```
4. Ensure the file permissions on the authorized_keys file are correct. SSH is particular about file permissions, and will refuse to work if they are incorrect.
   ```bash
   chmod 600 ~/.ssh/authorized_keys
   ```
5. Retrieve the contents of the private key. This can be copied into the RN150 appliance when creating an SSH credential entry.
   ```bash
   cat ~/.ssh/id_rsa
   ```

Testing Sudo Configuration

This is an example series of commands for testing the sudo configuration. It assumes that the user account used for collection is named 'risc'.

Task | To test Sudo configuration:
--- | ---
1. Log in to the account
   ```bash
   su - risc
   ```
2. Run the built-in sudo configuration test to confirm that the sudoers syntax is valid and the user account has basic access to run sudo.
   ```bash
   sudo -v
   ```
3. Run the true command under sudo to confirm that the account is permitted to execute a command. The true command is used by the SSH Collection Module to test access to sudo.
   ```bash
   sudo true
   ```
Basic Example Sudo Configuration

This is an example configuration for a Linux system that broadly grants the ability to execute commands using sudo. This is the least secure option, but is easy to implement and maintain. It assumes that the user account used for collection is named 'risc'.

# remove the TTY restriction for this user
Defaults:risc !requiretty

# allow the user to issue commands as root without a password
risc ALL=(root) NOPASSWD: ALL

Advanced Example Sudo Configuration

This is an example configuration for a Linux system that explicitly defines the commands that are permitted to be executed through sudo. It assumes that the user account used for collection is named 'risc'. The commands are specified by their absolute paths, and may differ between OS distributions and/or versions. This example is for illustrative purposes only. It may not contain all commands requiring sudo. See the Command Reference below for an up-to-date list.

# remove the TTY restriction for this user
Defaults:risc !requiretty

# allow specific commands permitted for the user
# backslashes are used to continue the configuration on a new line for clarity
risc ALL=(root) NOPASSWD: \
  /bin/true, \
  /sbin/ifconfig, \
  /bin/df -P, \
  /bin/netstat --inet --inet6 -n -p -a -t, \
  /sbin/fdisk -l, \
  /bin/cat /sys/devices/virtual/dmi/id/*, \
  /usr/sbin/dmidecode --type system, \
  /usr/sbin/dmidecode --type chassis, \
  /usr/sbin/dmidecode --type bios

SSH Collection Module Command Reference

The following tables describe the commands that may be issued by the SSH Collection module. The commands that are issued depend on the operating system. Not all listed commands are issued against every system. Certain commands are only issued in the case that a more preferable command is not available, and certain commands may be specific to a particular OS distribution and/or version.

The Privileged column describes whether the command will be issued using the sudo utility to elevate privileges. Commands listed as ‘fallback’ are first attempted without sudo, and then attempted with sudo if the first attempt fails.

- SSH Collection Module Linux Command Reference
- SSH Collection Module AIX Command Reference
## SSH Collection Module Linux Command Reference

The following table contains the Linux command reference for the SSH Collection Model.

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo true</td>
<td>Yes</td>
<td>Immediately returns successfully.</td>
<td>Used to validate access to the sudo utility.</td>
</tr>
<tr>
<td>uname -a</td>
<td></td>
<td>Returns all elements in the system utsvname struct.</td>
<td>Used for a full descriptive string for the system.</td>
</tr>
<tr>
<td>uname -s</td>
<td></td>
<td>Returns the operating system name.</td>
<td>Used for OS detection.</td>
</tr>
<tr>
<td>uname -r</td>
<td></td>
<td>Returns the operating system release version.</td>
<td>Used for kernel version detection.</td>
</tr>
<tr>
<td>uname -p</td>
<td></td>
<td>Returns the hardware platform type.</td>
<td>Used for system architecture detection.</td>
</tr>
<tr>
<td>uname -m</td>
<td></td>
<td>Returns the hardware machine type.</td>
<td>Used for system architecture detection.</td>
</tr>
<tr>
<td>uname -n</td>
<td></td>
<td>Returns the system hostname.</td>
<td>Used for hostname detection.</td>
</tr>
<tr>
<td>cat /etc/os-release</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used during OS distribution detection.</td>
</tr>
<tr>
<td>cat /etc/oracle-release</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used during OS distribution detection.</td>
</tr>
<tr>
<td>cat /etc/redhat-release</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used during OS distribution detection.</td>
</tr>
<tr>
<td>find /etc -type f</td>
<td>grep -e '[-<em>]release$' -e '[-</em>]version$'</td>
<td>Finds files matching a search pattern.</td>
<td>Used during distribution detection, to find distribution information files not listed above.</td>
</tr>
<tr>
<td>cat $file</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used for to retrieve the contents of a distribution file discovered by the command above. The filename must be recognized before operating on it.</td>
</tr>
<tr>
<td>cat /proc/uptime</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system uptime.</td>
</tr>
<tr>
<td>w -h</td>
<td></td>
<td>Returns details of logged in users.</td>
<td>Used to retrieve the number of current user logins.</td>
</tr>
</tbody>
</table>
### Table 2-11 • Linux Command Reference for SSH Collection Model

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>cat /proc/cpuinfo</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve CPU topology.</td>
</tr>
<tr>
<td>cat /proc/meminfo</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve system memory size and utilization.</td>
</tr>
<tr>
<td>ps axwww --no-headers -o pid,cputime,rsz,command</td>
<td></td>
<td>Returns details on running processes.</td>
<td>Used to retrieve a list of running processes.</td>
</tr>
<tr>
<td>sudo ifconfig -a</td>
<td>Yes</td>
<td>Returns details on network interfaces.</td>
<td>Used to retrieve details on all network interfaces.</td>
</tr>
<tr>
<td>sudo ifconfig $interface</td>
<td>Yes</td>
<td>Returns details on network interfaces.</td>
<td>Used to retrieve details on a specific network interface, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>cat /sys/class/net/$interface/ifindex</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the network interface index number, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>cat /sys/class/net/$interface/operstate</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the network interface physical state, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>cat /sys/class/net/$interface/mtu</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the network interface MTU, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>cat /sys/class/net/$interface/speed</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the network interface bps rate, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>readlink /sys/class/net/$interface/device/driver/module</td>
<td></td>
<td>Canonicalizes the path of a symlink or file.</td>
<td>Used to retrieve the network interface driver, where $interface is the name of a previously collected network interface.</td>
</tr>
<tr>
<td>lsblk -dnb --output NAME,MAJ:MIN,SIZE,MODEL</td>
<td></td>
<td>Returns details on disks and partitions.</td>
<td>Used to retrieve physical disk details</td>
</tr>
</tbody>
</table>
### Table 2-11 • Linux Command Reference for SSH Collection Model

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sudo fdisk -l</code></td>
<td>Yes</td>
<td>Lists or configures disk partitions.</td>
<td>Used to retrieve physical disk details if lsblk is unavailable.</td>
</tr>
<tr>
<td><code>cat /sys/block/$device/device/model</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the disk model string, if available, where $device is the name of a previously collected disk device.</td>
</tr>
<tr>
<td><code>cat /proc/partitions</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve disk partition details.</td>
</tr>
<tr>
<td><code>mount</code></td>
<td>Fallback</td>
<td>Lists mounted filesystems.</td>
<td>Used to retrieve a list of mounted filesystems.</td>
</tr>
<tr>
<td><code>sudo df -P</code></td>
<td>Yes</td>
<td>Lists filesystem utilization details.</td>
<td>Used to retrieve filesystem utilization details.</td>
</tr>
<tr>
<td><code>vmstat -w -S K 1 2</code></td>
<td></td>
<td>Lists various system performance details.</td>
<td>Used to retrieve system performance details. It may be used without the -w flag for some systems. The command produces two metric reports with a one second wait between them.</td>
</tr>
<tr>
<td><code>cat /proc/diskstats</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve disk performance details.</td>
</tr>
<tr>
<td><code>sudo netstat --inet --inet6 -n -p -a -t</code></td>
<td>Yes</td>
<td>Lists open sockets.</td>
<td>Used to retrieve network connections.</td>
</tr>
<tr>
<td><code>cat /proc/net/dev</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve various network subsystem statistics.</td>
</tr>
<tr>
<td><code>ls /sys/devices/virtual/dmi/id</code></td>
<td></td>
<td>Lists directory contents.</td>
<td>Used to check for the existence of hardware platform data using sysfs.</td>
</tr>
<tr>
<td><code>cat /sys/devices/virtual/dmi/id/sys_vendor</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system hardware vendor from sysfs.</td>
</tr>
<tr>
<td><code>cat /sys/devices/virtual/dmi/id/product_name</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system product name from sysfs.</td>
</tr>
<tr>
<td><code>cat /sys/devices/virtual/dmi/id/product_version</code></td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system product version from sysfs.</td>
</tr>
<tr>
<td><code>sudo cat /sys/devices/virtual/dmi/id/product_serial</code></td>
<td>Yes</td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system product serial number from sysfs.</td>
</tr>
</tbody>
</table>
Table 2-11 • Linux Command Reference for SSH Collection Model

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo cat /sys/devices/virtual/dmi/id/product_uuid</td>
<td>Yes</td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the system product UUID from sysfs.</td>
</tr>
<tr>
<td>cat /sys/devices/virtual/dmi/id/chassis_vendor</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the chassis vendor from sysfs.</td>
</tr>
<tr>
<td>cat /sys/devices/virtual/dmi/id/chassis_version</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the chassis version from sysfs.</td>
</tr>
<tr>
<td>sudo cat /sys/devices/virtual/dmi/id/chassis_serial</td>
<td>Yes</td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the chassis serial number from sysfs.</td>
</tr>
<tr>
<td>cat /sys/devices/virtual/dmi/id/bios_vendor</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the BIOS vendor from sysfs.</td>
</tr>
<tr>
<td>cat /sys/devices/virtual/dmi/id/bios_version</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the BIOS version from sysfs.</td>
</tr>
<tr>
<td>cat /sys/devices/virtual/dmi/id/bios_date</td>
<td></td>
<td>Emits the contents of a file.</td>
<td>Used to retrieve the BIOS build date from sysfs.</td>
</tr>
<tr>
<td>which dmidecode</td>
<td></td>
<td>Lists the location of an executable file.</td>
<td>Used to check for the existence of the dmidecode utility, as a fallback if sysfs is unavailable.</td>
</tr>
<tr>
<td>sudo dmidecode --type system</td>
<td>Yes</td>
<td>Retrieves hardware info from DMI.</td>
<td>Used to retrieve system hardware product information.</td>
</tr>
<tr>
<td>sudo dmidecode --type chassis</td>
<td>Yes</td>
<td>Retrieves hardware info from DMI.</td>
<td>Used to retrieve chassis hardware information.</td>
</tr>
<tr>
<td>sudo dmidecode --type bios</td>
<td>Yes</td>
<td>Retrieves hardware info from DMI.</td>
<td>Used to retrieve BIOS information.</td>
</tr>
<tr>
<td>sh -c &quot;(rpm -qf /bin/sh &gt;&gt;/dev/null 2&gt;&amp;1 &amp;&amp; echo rpm)</td>
<td></td>
<td>(dpkg -S /bin/sh &gt;&gt;/dev/null 2&gt;&amp;1 &amp;&amp; echo dpkg)</td>
<td></td>
</tr>
<tr>
<td>rpm -qa --queryformat &quot;META|^{NAME}|^{EPOCH}|^{VERSION}|^{RELEASE}|^{SUMMARY}|^{Filenames}| / / \n</td>
<td>grep -E &quot;META|^| / / $</td>
<td>^.*bin/&quot;</td>
<td></td>
</tr>
<tr>
<td>dpkg-query --show --showformat=&quot;META|^{binary:Package}|^{Version}|^{db:Status- Abbrev}|^{binary:Summary}\n</td>
<td></td>
<td>Lists metadata for installed software packages.</td>
<td>Used to retrieve a complete list of installed packages for systems using dpkg as a package manager.</td>
</tr>
</tbody>
</table>
Table 2-12 • AIX Command Reference for SSH Collection Model

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo true</td>
<td>Yes</td>
<td>Immediately returns</td>
<td>Used to validate access to the sudo utility.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>successfully.</td>
<td></td>
</tr>
<tr>
<td>uname -a</td>
<td></td>
<td>Returns all elements in the</td>
<td>Used for a full descriptive string for the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system utsname structure.</td>
<td></td>
</tr>
<tr>
<td>uname -s</td>
<td></td>
<td>Returns the operating system</td>
<td>Used for OS detection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name.</td>
<td></td>
</tr>
<tr>
<td>uname -r</td>
<td></td>
<td>Returns the operating system</td>
<td>Used for OS version detection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minor version</td>
<td></td>
</tr>
<tr>
<td>uname -v</td>
<td></td>
<td>returns the operating system</td>
<td>Used for OS version detection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>major version</td>
<td></td>
</tr>
<tr>
<td>uname -p</td>
<td></td>
<td>Returns the hardware</td>
<td>Used for system architecture detection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>platform type.</td>
<td></td>
</tr>
<tr>
<td>uname -n</td>
<td></td>
<td>Returns the system hostname.</td>
<td>Used for hostname detection.</td>
</tr>
<tr>
<td>lsdev</td>
<td></td>
<td>Returns a list of devices on</td>
<td>Used to determine devices eligible for further inspection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the system.</td>
<td></td>
</tr>
<tr>
<td>lsdev -Cc if</td>
<td></td>
<td>Returns a list of network</td>
<td>Used to retrieve list of network devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interfaces on the system.</td>
<td></td>
</tr>
<tr>
<td>ps -o etime= -p1</td>
<td></td>
<td>Returns details on running</td>
<td>Used to derive the system uptime, by determining the elapsed time since the init</td>
</tr>
<tr>
<td></td>
<td></td>
<td>processes.</td>
<td>process started.</td>
</tr>
<tr>
<td>w -h</td>
<td></td>
<td>Returns details of logged in</td>
<td>Used to retrieve the number of current user logins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Privileged</td>
<td>Command Operation</td>
<td>Reason for Use</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lsattr -E -l sys0 -a realmem</td>
<td></td>
<td>Returns details on a system logical device.</td>
<td>Used to determine the size of system memory.</td>
</tr>
<tr>
<td>ps -e -o pid,cputime,rssize,args</td>
<td></td>
<td>Returns details on running processes.</td>
<td>Used to retrieve a list of running processes.</td>
</tr>
<tr>
<td>lsattr -E -l procN</td>
<td></td>
<td>Returns details on a system logical device.</td>
<td>Used to retrieve CPU details, where N is a CPU device index seen from lsdev.</td>
</tr>
<tr>
<td>ifconfig -a</td>
<td></td>
<td>Returns details on network interfaces.</td>
<td>Used to retrieve details on network interfaces.</td>
</tr>
<tr>
<td>entstat $device</td>
<td></td>
<td>Returns statistics on an ethernet device.</td>
<td>Used to retrieve statistics for ethernet devices, where $device is the name of an ethernet device.</td>
</tr>
<tr>
<td>lsattr -E -l $device -a state,netaddr,netmask,netaddr6,mtu</td>
<td></td>
<td>Returns details on a system logical device.</td>
<td>Used to retrieve statistics for ethernet devices, where $device is the name of an ethernet device.</td>
</tr>
<tr>
<td>sudo getconf DISK_SIZE /dev/$device</td>
<td>Fallback</td>
<td>Returns the value of a system configuration variable.</td>
<td>Used to retrieve the size of physical disks reported by lsdev. The disks may have access restrictions in some configurations that require privilege elevation.</td>
</tr>
<tr>
<td>lsfs</td>
<td>Fallback</td>
<td>Returns filesystem details.</td>
<td>Used to retrieve a list of filesystems.</td>
</tr>
<tr>
<td>sudo df -Pk</td>
<td>Fallback</td>
<td>Returns filesystem details.</td>
<td>Used to retrieve filesystem size and utilization. Normally, df doesn’t require elevated privileges. However, in some cases, certain file-systems cannot be shown without, and if df returns an error, it is attempted with elevated privileges.</td>
</tr>
<tr>
<td>lspp -lq</td>
<td>grep -v '^#Path'</td>
<td></td>
<td>Returns a list of installed software.</td>
</tr>
</tbody>
</table>
Troubleshooting Introduction

It is highly recommended to test SSH access and operation prior to issuing a Discovery scan, to ensure that the hosts are configured correctly for the SSH Collection Module. This can be performed from the SSH credentials section on the RN150 Virtual Appliance, which will validate the ability of the RN150 Virtual Appliance to connect to the target hosts at the

<table>
<thead>
<tr>
<th>Command</th>
<th>Privileged</th>
<th>Command Operation</th>
<th>Reason for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmstat 1 2</td>
<td></td>
<td>Returns details on system utilization.</td>
<td>Used to retrieve various system utilization statistics. It produces two metric reports, with a one second wait between them.</td>
</tr>
<tr>
<td>vmstat -v</td>
<td></td>
<td>Returns details on virtual memory utilization.</td>
<td>Used to retrieve detailed information on virtual memory utilization.</td>
</tr>
<tr>
<td>pagesize</td>
<td></td>
<td>Returns the size of a virtual memory page.</td>
<td>Used to convert virtual memory page utilization to byte-sizes.</td>
</tr>
<tr>
<td>iostat -Dl 1 1</td>
<td></td>
<td>Returns statistics on system I/O activity.</td>
<td>Used to retrieve statistics on system I/O.</td>
</tr>
<tr>
<td>sudo lsof -i -nP</td>
<td>Fallback</td>
<td>Returns a list of open file descriptors.</td>
<td>Used to retrieve details of open network sockets. Normally, lsfs doesn't require privilege elevation, however, in some cases it seems it may. To avoid interfering with engagements where this is working and not configured for privilege elevation we first try without and then fall back to try with.</td>
</tr>
</tbody>
</table>

**SSH Collection Module Troubleshooting**

Information about SSH Collection Module troubleshooting is organized in the following sections:

- Troubleshooting Introduction
- Troubleshooting Command Reference
- Troubleshooting Command Suite
- SSH Collection Module Error Messages
network level, and will test the native operation of the SSH Collection Module. However, it may be desired to perform more manual tests from another host in the environment, allowing the enablement of debugging options in SSH for deeper analysis.

Testing from the RN150 Virtual Appliance is covered above in the credential entry sections. This section will cover the manual tests that can be performed for deeper analysis of the configuration.

To test SSH access to a target host, first log in to another host in the environment that provides an SSH client. This will be referred to as the "local" host, while the host that is being connected to is referred to as the "target". In the following examples, the target is assumed to have an IP address of 10.0.0.2, and the username of the account we are connecting to is "risc".

The general structure of the SSH command, in manpage format, is as follows:

```
ssh [flags] [authentication-flags] <username>@<host-IP> "<command>"
```

A breakdown of this command is as follows:

**Table 2-13 • SSH Command Breakdown**

<table>
<thead>
<tr>
<th>Component</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>literal</td>
<td>The ssh client binary</td>
</tr>
<tr>
<td>[flags]</td>
<td>optional</td>
<td>General flags to control the ssh client behavior</td>
</tr>
<tr>
<td>[authentication-flags]</td>
<td>optional</td>
<td>Controls explicit authentication behavior</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>replace</td>
<td>The username of the account we are connecting with</td>
</tr>
<tr>
<td>&lt;host-IP&gt;</td>
<td>replace</td>
<td>The IP address of the target host</td>
</tr>
<tr>
<td>&quot;&lt;command&gt;&quot;</td>
<td>replace</td>
<td>The command to issue on the target host, contained in single or double quotes</td>
</tr>
</tbody>
</table>

**Troubleshooting Command Reference**

Normally, the ssh client is invoked without the final argument shown above, which performs a login to the target host into an interactive shell session. When invoked with the optional command argument, this causes the ssh client to only invoke that command in a non-interactive fashion. This is an important component of the troubleshooting process, as the use of the command argument will replicate the behavior of the SSH Collection Module. It also provides a test for the behavior described above; an interactive session will allocate a TTY terminal device, while the non-interactive execution of a single command will not. This allows testing the sudo configuration, which will often require a TTY device associated with the user session invoking it.

When performing troubleshooting to determine the cause of an authentication failure experienced by the SSH Collection Module, the `-v` flag can be given to the ssh client to cause it to emit extra verbose debugging output. This flag can be given multiple times to cause the ssh client to emit more information. It is highly recommended to use this flag when performing troubleshooting.
Depending on the type of authentication being utilized, the authentication-flags field may need to be used to cause the client to specifically use the type of authentication desired, as well as the specific authentication credentials to be used.

Table 2-14 • Authentication Flags

<table>
<thead>
<tr>
<th>Type of Authentication</th>
<th>authentication-flags Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password or keyboard-interactive authentication</td>
<td>If using password or keyboard-interactive authentication, this can be specified as, for example:</td>
</tr>
<tr>
<td></td>
<td>-o PreferredAuthentications=&quot;password&quot;</td>
</tr>
<tr>
<td>publickey authentication</td>
<td>If using publickey authentication, this would be:</td>
</tr>
<tr>
<td></td>
<td>-o PreferredAuthentications=&quot;publickey&quot;</td>
</tr>
<tr>
<td>publickey authentication to specify which key the client utilizes for authentication attempts</td>
<td>If using publickey authentication, to specify which key the client utilizes for authentication attempts, the following could be used, for example:</td>
</tr>
<tr>
<td></td>
<td>-i /home/risc/key</td>
</tr>
<tr>
<td>Simple connection test using password authentication to the target host to validate the connection</td>
<td>To perform a simple connection test using password authentication to the target host to validate the connection, authentication, and ability to issue a simple command:</td>
</tr>
<tr>
<td></td>
<td>ssh -v -o PreferredAuthentications=&quot;password&quot; risc@10.0.0.2 &quot;true&quot;</td>
</tr>
<tr>
<td>Simple connection test using publickey authentication to the target host to validate the connection</td>
<td>To test the same with publickey authentication:</td>
</tr>
<tr>
<td></td>
<td>ssh -v -o PreferredAuthentications=&quot;publickey&quot; -i /home/risc/key risc@10.0.0.2 &quot;true&quot;</td>
</tr>
<tr>
<td>Testing the availability and configuration of sudo</td>
<td>Testing the availability and configuration of sudo is of primary importance, as this is often the main reason for a failure to bring a host into inventory:</td>
</tr>
<tr>
<td></td>
<td>ssh -v risc@10.0.0.2 'sudo ifconfig -a'</td>
</tr>
</tbody>
</table>

Troubleshooting Command Suite

The following is a series of commands that will validate the enablement of the SSH Collection Module for a given host. When a support case is opened, a support engineer will likely request the results of the follow series of commands. In this case, it is not expected that legitimate customer data that results from a successful command be sent to support, but any error messages produced will be expected to be provided. These error messages may be cleaned to the extent that usernames or other data deemed private may be removed, however extensive redaction of data may result in difficulty providing insight into the failure.

In these examples, each ssh command is followed by a shell command to print the exit status of the previously issued command. Replace the user and IP elements in angle brackets with the username being utilized and the IP address of the target host.
**Linux Targets**

For Linux targets, use the following to validate the enablement of the SSH Collection Module for a given host.

```bash
ssh -v <user>@<IP> 'true'  
echo $?  
ssh -v <user>@<IP> 'sudo true'  
echo $?  
ssh -v <user>@<IP> 'uname -s'  
echo $?  
ssh -v <user>@<IP> 'sudo ifconfig -a'  
echo $?  
ssh -v <user>@<IP> 'sudo df -P'  
echo $?  
ssh -v <user>@<IP> 'uname -s'  
echo $?  
ssh -v <user>@<IP> 'lsdev'  
echo $?  
ssh -v <user>@<IP> 'lsattr -E -l sys0 -a realmem'  
echo $?  
ssh -v <user>@<IP> 'df -P'  
echo $?  
ssh -v <user>@<IP> 'df -P'  
echo $?  
ssh -v <user>@<IP> 'lsof -i -nP'  
echo $?  
ssh -v <user>@<IP> 'netstat -an -f inet'  
echo $?
```

**AIX Targets**

For AIX targets, use the following to validate the enablement of the SSH Collection Module for a given host.

```bash
ssh -v <user>@<IP> 'true'  
echo $?  
ssh -v <user>@<IP> 'sudo true'  
echo $?  
ssh -v <user>@<IP> 'uname -s'  
echo $?  
ssh -v <user>@<IP> 'lsdev'  
echo $?  
ssh -v <user>@<IP> 'lsattr -E -l sys0 -a realmem'  
echo $?  
ssh -v <user>@<IP> 'df -P'  
echo $?  
ssh -v <user>@<IP> 'df -P'  
echo $?  
ssh -v <user>@<IP> 'lsof -i -nP'  
echo $?  
ssh -v <user>@<IP> 'netstat -an -f inet'  
echo $?
```
SSH Collection Module Error Messages

Understanding the error messages received when testing the credential, through the RN150 Virtual Appliance credential testing facility or through manual testing, is key to pinpointing the problem. Due to the nature of the ssh client/server interaction, it is common to receive non-error related text in the error message. This includes any banner text returned to the client by the server, as well as a message indicating that the server’s host keys have been added to the list of known hosts. These elements of the error can be ignored.

The following is a non-exhaustive list of common error messages, and their meaning:

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Context</th>
<th>Description of behavior</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to determine operating system using command 'uname -s'</td>
<td>credential testing</td>
<td>The 'uname -s' command was not successful. The target device does not support this command, or the command was otherwise unable to execute. The successful completion of this command is a strict requirement for participation in the SSH Collection Module.</td>
<td>• Confirm the target operating system is supported by the SSH Collection Module&lt;br&gt;• Ensure the 'uname' command exists and the user account can execute it&lt;br&gt;• Configure the device for SNMP collection</td>
</tr>
<tr>
<td>Unsupported Operating System</td>
<td>credential testing</td>
<td>The target operating system is not supported; the target device is not eligible for participation in the SSH Collection Module</td>
<td>• Review the supported operating systems above&lt;br&gt;• Configure the device for SNMP collection</td>
</tr>
<tr>
<td>Successfully connected, but sudo validation failed</td>
<td>credential testing</td>
<td>Connection and authentication was successful, but the user account was unable to utilize sudo</td>
<td>• Review sudo configuration&lt;br&gt;• Review the sudo logs</td>
</tr>
<tr>
<td>Connection refused</td>
<td>connection</td>
<td>The ssh client connection was not successful. This could mean that:</td>
<td>• Ensure ssh server is running on host&lt;br&gt;• Ensure ssh server is listening on expected TCP port on the host&lt;br&gt;• Ensure local firewall is not blocking&lt;br&gt;• Ensure network ACLs are not blocking</td>
</tr>
<tr>
<td>No route to host</td>
<td>connection</td>
<td>The RN150 has no route to the target IP address</td>
<td>• Review network configuration on the RN150&lt;br&gt;• Review VLAN configurations&lt;br&gt;• Review routing to that subnet</td>
</tr>
</tbody>
</table>
Table 2-15 • SSH Collection Module Error Messages (cont.)

<table>
<thead>
<tr>
<th>Error Text</th>
<th>Context</th>
<th>Description of behavior</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission denied (...)</td>
<td>authentication</td>
<td>The credentials offered by the client were refused by the server. This could mean that:</td>
<td>• Ensure credential was entered correctly in the RN150</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the username is not a valid user on the target</td>
<td>• Ensure username exists on the target</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the user is not permitted</td>
<td>• Review ssh access controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the password is invalid for the user</td>
<td>• Review authentication configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the key was corrupted or an invalid or unknown type</td>
<td>• Ensure private key is not encrypted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• file permissions on files related to authentication (keys, configuration files, etc) were not correct</td>
<td>• Review file permissions on target</td>
</tr>
</tbody>
</table>

This message is followed by a list, in parentheses, of authentication methods announced by the server.

Connection reset by peer  any  The target ssh server suddenly aborted the connection. This is a generic error that has a large number of possible causes.

Often, this is a particular form of refused connection, where the initial stages of the connection were successful but additional access controls determined that the connection cannot continue.

This could also be due to one of the following:

• The TCP session was lost
• The client and server were unable to negotiate compatible session keys and MACs
• The server only supports version 1 of the SSH protocol
• Server is unable to handle an additional connection, or to fork a process for the requested command

• Ensure that hosts.deny, hosts.allow, or similar are configured to permit the connection
• Ensure that the ssh server supports version 2 of the protocol
• Review server logs on the target
Database Module

Database servers are some of the most complicated nodes in a network often because they are shared across many applications. The database module collects information about the connectivity of each schema within your database host, and integrates client connections into our overall connectivity architecture. Assessments with the Database Module active are able to map server dependency to the schema level so an organization can understand what particular data sets an application may be dependent on.

- Overview of the Database Module
- Using the Database Module
- Queries Run By the Database Module

Overview of the Database Module

The Database Module has been released as a preview feature.

We support connectivity analytics for:

- MySQL
- Microsoft SQL Server (2008 and later)
- Oracle
Unlike most RISC data collection modalities, the Database Module does not have an automated discovery process and must be manually configured. In order for collection to take place, the DB host information and an account with adequate permissions must be manually provided into the RN150. We recommend that a temporary dedicated user is created and used for analyzing the database. The required permissions for the temporary user are outlined below. We also recommend that the user is removed after the assessment ends.

**Note** • Oracle Database users: please note that due to the way Oracle manages its dataspaces, we do collect usernames in their role as database schemas.

### Using the Database Module

To use the database module, perform the following steps:

<table>
<thead>
<tr>
<th>Task</th>
<th>To use the Database Module:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Go to the RN-150 Dashboard and locate the “Additional Credentials” page at the bottom of the list.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Credential Type drop-down menu, select “database.”</td>
</tr>
<tr>
<td>3.</td>
<td>Entered the connection information for your first database server, and hit “Add.”</td>
</tr>
<tr>
<td>4.</td>
<td>Enter the server’s IP and hit “test.” If the test is unsuccessful, press “cancel” to verify that the credentials were added correctly and retry.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter and test connection information for each individual database server you would like to have analyzed. Oracle cluster database users should enter each server in a cluster separately and provide a direct connection to each server.</td>
</tr>
</tbody>
</table>

### Account Permissions

The Database Module requires the following permissions:

**Table 2-16 • Database Module Account Permissions**

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>The account provided must have SHOW DATABASES and SHOW PROCESS privileges. It also requires select privileges on <code>*.*</code>.</td>
</tr>
<tr>
<td>MS SQL Server</td>
<td>The account provided must have VIEW SERVER STATE, VIEW DATABASE STATE, and VIEW ANY DATABASE permissions.</td>
</tr>
<tr>
<td>Oracle Database</td>
<td>The account provided must have select privileges on V$INSTANCE and V$SESSION as well as on the following DBA tables: DBA_USERS, DBA_TABLES, DBA_INDEXES, DBA_OBJECTS, DBA_SEGMENTS, and DBA_LOBS.</td>
</tr>
</tbody>
</table>
Queries Run By the Database Module

The specific queries run during the course of inventory and performance analysis are specific to the DBMS.

- **MySQL**
- **MS SQL Server**
- **Oracle Database**

### MySQL

The following queries are run by an MySQL database:

```sql
select @@hostname h, @@version v
SELECT SCHEMA_NAME FROM information_schema.schemata
SELECT host, db, command, state, time FROM information_schema.processlist
select db, count(distinct(user)) userCount from information_schema.processlist group by db
SELECT *, unix_timestamp(create_time) ct, unix_timestamp(update_time) ut, unix_timestamp(check_time) cht FROM INFORMATION_SCHEMA.TABLES
```

### MS SQL Server

The following queries are run by an MS SQL Server database:

```sql
select SERVERPROPERTY ('ProductVersion') v, SERVERPROPERTY ('MachineName') h
SELECT name, database_id, create_date FROM sys.databases
SELECT name s FROM sys.databases
SELECT conn.client_net_address,
    conn.client_tcp_port,
    sess.status,
    sess.last_request_start_time,
    DB_NAME(sess.database_id) AS db
FROM sys.dm_exec_sessions sess
LEFT JOIN sys.dm_exec_connections conn
    ON sess.session_id=conn.session_id
WHERE sess.is_user_process=1
select DB_NAME(database_id) as db, count(distinct(login_name)) userCount from sys.dm_exec_sessions group
by DB_NAME(database_id)
select count(distinct(login_name)) userCount from sys.dm_exec_sessions
```

```sql
select
t.name as tableName,
s.name as secondarySchema,
datediff(s, '1970-01-01 00:00:00', max(t.create_date)) as createDate,
datediff(s, '1970-01-01 00:00:00', max(t.modify_date)) as updateDate,
max(p.rows) as RowCounts,
sum(a.total_pages*8) as totalSpaceKB,
sum(a.used_pages*8) as usedSpaceKB,
sum(case when i.index_id < 2 then a.data_pages*8 else 0 end) as dataSpaceKB,
sum(a.used_pages*8)-sum(case when i.index_id < 2 then a.data_pages*8 else 0 end) as indexSpaceKB
from $schema.sys.tables t
inner join $schema.sys.indexes i on t.object_id = i.object_id
inner join $schema.sys.partitions p on i.object_id = p.object_id and i.index_id = p.index_id
```
inner join $schema.sys.allocation_units a on p.partition_id = a.container_id
inner join $schema.sys.schemas s on t.schema_id=s.schema_id

group by t.name, s.name

**Oracle Database**

The following queries are run by an Oracle database:

```
SELECT HOST_NAME H, VERSION V FROM V$INSTANCE
SELECT username FROM dba_users u WHERE EXISTS (SELECT 1 FROM dba_objects o WHERE o.owner = u.username)
SELECT MACHINE, PORT, SCHEMANAME, STATUS, COMMAND, LAST_CALL_ET FROM v$session WHERE username IS NOT NULL

select schemaname DB, count(distinct(user)) USERCOUNT from v$session group by schemaname

select count(distinct(user)) userCount from v$session

select table_name, owner, sum(decode(type,'table',bytes))/1024 tableKB,
sum(decode(type,'index',bytes))/1024 indexKB, sum(decode(type,'lob',bytes))/1024 lobKB,
sum(bytes)/1024 totalKB, sum(num_rows) numRows, max(last_anal) last_anal,
max(created) created, max(updated) updated, max(tbs) tablespace,
sum(decode(type,'table','bytes','lob',bytes))/1024 totalDataKB,
sum(decode(type,'index','bytes','lobidx',bytes))/1024 totalIdxKB
from
select t.table_name table_name, 'table' type, t.owner, s.bytes, t.num_rows,
t.last_analyzed last_anal, o.created created, o.last_ddl_time updated, t.tablespace_name tbs
from dba_tables t left join dba_segments s
on s.segment_name=t.table_name and s.owner=t.owner
left join dba_objects o on t.table_name=o.object_name and t.owner=o.owner
where s.segment_type in ("TABLE","TABLE PARTITION","TABLE SUBPARTITION") or s.segment_type is null
union all select i.table_name table_name, 'index' type, i.owner, s.bytes, 0 num_rows,
null last_anal, null created, null updated, null tbs
from dba_segments s inner join dba_indexes i
on i.index_name = s.segment_name and s.owner = i.owner
where s.segment_type in ("INDEX","INDEX PARTITION","INDEX SUBPARTITION")
union all select l.table_name, 'lob' type, l.owner, s.bytes, 0 num_rows, null last_anal,
null created, null updated, null tbs
from dba_lobs l inner join dba_segments s on l.segment_name = s.segment_name and l.owner = s.owner
where s.segment_type in ("LOBSEGMENT","LOB PARTITION")
union all select l.table_name, 'lobidx' type, l.owner, s.bytes, 0 num_rows, null last_anal,
null created, null updated, null tbs
from dba_lobs l inner join dba_segments s on l.index_name = s.segment_name and s.owner = l.owner
where s.segment_type = 'LOBINDEX'

```
Load Balancers

Environments that contain load balancers can yield confusing or incomplete data if the load balancer’s self-IPs are not properly inventoried. F5 load balancers support interface collection using our standard inventory process via either SNMP or SSH (requires administrator-level credentials), while Netscaler is only collectible via SNMP.

In order to inventory your F5 or Netscaler load balancer, please make sure that:

- SNMP is enabled on the load balancer (if using SNMP, which is mandatory for Netscaler)
- You provide us with a valid SNMP credential or, if using SSH (F5 only), provide us with Administrator-level credentials
- The management IP of the load balancer is within scope of the subnets to be scanned
- For best results, please make sure that the load-balanced application servers in your environment are also in scope and accessible via their own IP addresses

During discovery/inventory we will assign all IPs owned by the load balancer (including VIPs) to itself. This will allow us to correctly map flows to and from the load balancer. We do not yet support the collection of connectivity data for the load balanced VIPs via either collection method. Please note that F5s will appear in your inventory as generic servers, while Netscalers will be inventoried as network devices.

AWS Collection Module

Information about the AWS Collection Module is organized in the following sections:

- Purpose and Requirements
- Performance Polling
- Visibility as Assets

Important The AWS Collection Module is deprecated. It is not available for new installations.

Purpose and Requirements

The AWS collection module provides inventory and performance data collection for entities hosted in the Amazon Web Services cloud (currently limited to EC2 instances). Data is requested by the RN150 appliance from the AWS API. As such, access to the AWS API must be provided from the RN150. An AWS access key and secret must be provided to the appliance and this credential must have the following permissions at a minimum:

IAM Minimum Policy Definition

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeElasticGpus"
            ],
```
The "Resource" element may be restricted in order to limit the scope of access. Instructions for creating a new IAM user account. After creating the account, you can attach a policy directly to that account using the JSON above.

Performance Polling

EC2 API calls (used for inventory data) are free, but there is a cost associated with the CloudWatch performance metric calls. To reduce this cost, we will perform data pull only once per day.

A separate API call must be made for each device, metric, and aggregation type being requested.

The metrics we collect are:

- CPUUtilization
- NetworkIn
- NetworkOut
- DiskReadBytes
- DiskReadOps
- NetworkPacketsIn
- NetworkPacketsOut
- DiskWriteBytes
- DiskWriteOps

The aggregation types are:

- Hourly
- Daily
- 95th percentile

This yields 27 API calls per device per day. Assuming that nothing else is using the CloudWatch API, the free 1,000,000 monthly calls would suffice for just over 1,200 instances. Beyond that, charges would be incurred (approximately $0.0081 per device per month based on $0.01/1000 calls).

Note  •  95th percentile metric is only available when detailed monitoring is enabled
**Important** • Per AWS documentation, with basic monitoring, the metric interval is 5 minutes. With detailed monitoring it is 1 minute. These assumptions are made when converting absolute metrics to per second units (eg network bytes in to KBps). Because of this, the monitoring state is checked at the beginning of performance collection. If the current state is different than the state when we last collected, we will update the state and not collect performance at this interval. There can still be a problem if the state is changed and changed back within an interval.

For instance:

- Device is set up for basic monitoring at the polling time of 00:00 on day 1
- At 02:00 on day 1, the device is changed to detailed monitoring
- At 20:00 on day 1, the device changes back to basic monitoring
- At 00:00 on day 2, we go to poll again and see no change

This will cause some metrics to be incorrect during the hours of 02:00 - 20:00. All metrics except CPUUtilization are affected.

**Visibility as Assets**

EC2 instances will appear in the list of virtual machines. Their device type will either be 'AWS EC2' or, if we were able to directly inventory the device as well, 'Virtual-AWS-other collection type' (eg 'Virtual-AWS-Generic Server' or 'Virtual-AWS-Windows Server').

**Performance Counter Disambiguation**

RISC Networks assessments collect data from a variety of sources within your IT environment. In addition to consuming this data throughout our platform to provide cutting edge analytics, we make aggregated performance data available to you directly in the Performance and Trending module. This document presents some low-level explanations and disambiguations regarding the source of some of the data you will encounter in our platform.

- Disambiguation / Clarification on Selected Counters
- Data Sources
- Sampled vs. Aggregate Data

**Disambiguation / Clarification on Selected Counters**

In this section, we provide some clarification on some of the subtleties of the performance counters we report.

- CPU Utilization
- Memory Usage
- Disk Read and Write Statistics
- Network IO
- CPU Active/Running (VMware only)
CPU Utilization

The percent and absolute CPU utilization of a given device may be collected directly from the device’s operating system (through WMI, SSH, or SNMP), and for virtual machines it may be reported by VMware (see Data Sources, below). When both metrics are present, you may notice a difference in the two. VMware’s view of CPU utilization includes the operational overhead of virtualization, so it is often higher than the value reported by the operating system. Conversely, at times of high host resource consumption, VMware may restrict a guest’s CPU access in a way that is not visible to the operating system, resulting in VMware reporting a lower CPU utilization than the host does.

Memory Usage

Please note that we collect a different representative metric for memory utilization from VMware than we do directly from the OS (see Data Sources, below). Operating systems report committed memory - the amount of memory currently reserved by processes, and thus unavailable to the OS. VMware, in contrast, reports the amount of memory actively being used by guest processes. Because processes may not be actively using all of the memory they have reserved, the two metrics are not exactly equivalent. However, both metrics play similar roles in our analytics.

Disk Read and Write Statistics

Counters relating to disk IO are generally estimated by sampling the absolute counters provided by the operating system twice, separated by a brief interval. For SSH and some 64-bit SNMP implementations, we will use a longer sampling window to improve convergence (see Sampled vs Aggregate Data, below).

Network IO

Data transmit and receive rates (both in packets and bytes) are estimated by sampling the absolute counters provided by the operating system twice, separated by a brief interval. For SSH and some 64-bit SNMP implementations, we will use a longer sampling window to improve convergence (see Sampled vs Aggregate Data, below).

Packets dropped and packets with errors are reported as an average number seen during the sampling window, rather than as a rate. Because 32-bit counters do not provide the same level of coverage for detecting interface errors and discards as 64-bit counters, we recommend against comparing interface errors and discards between different devices. An increase or decrease in this statistic for a given device is worthy of note, and any value above 0 for these counters may be indicative of a problem.

CPU Active/Running (VMware only)

These counters are reported by VMware as a percentage, but please be aware that they are reported as the sum of the percent utilization of each logical core. This means that the total can exceed 100% for systems with multiple logical cpu cores.

Data Sources

We collect data about the state of the hosts and network devices in your system via a variety of methods: WMI, SSH, SNMP, VMware’s API, Netflow, database metadata, etc. We may collect against the same device using multiple collection methods. In order to distinguish between data about a virtualized server gathered using VMware’s API and data collected directly from that server’s operating system (through WMI, SSH, or SNMP), we may refer separately to the server’s VMware-sourced data and its data collected directly from the device’s OS. While the metrics collected are typically ways of measuring the same property of the system in question, they can differ from each other due to differences in data availability, collection interval, or sampling method.
For the purposes of cloud cost estimation, we prefer data collected from VMware if both that and directly-collected data were available throughout the assessment’s collection period.

**Sampled vs. Aggregate Data**

Most of our performance data is sampled: we poll each device once per collection interval (not more than once every five minutes). Many metrics and collection types report the instantaneous value of relevant performance metrics at the time of collection (e.g. a server with 25% memory usage at a given point in time); we report the average value of these metrics observed each hour of collection. Because we do not collect continuously, observed values are approximate; we recommend collecting for at least a month to reduce the impact of sampling error.

Some metrics, however, are recorded by operating systems as a count of events since system restart (or counter rollover). When the counter is stored as a 32-bit integer, we will measure the rate of events by polling the absolute counter twice within a short period, and extrapolate from this sampled rate to determine the average overall rate of events. With enough data points, these sampled values should converge towards the “true” average. When the operating system provides 64-bit counters (SSH and some SNMP implementations), we are able to calculate the number of events between polling intervals, effectively collecting events from the whole interval rather than extrapolating an approximate rate from a sample.

**ServiceNow Configuration and User Guide**

This section describes how to install, configure, and use the Foundation and CloudScape ServiceNow (SNOW) plugin.

- **Intended audience**—The reader of the Foundation and CloudScape ServiceNow (henceforth referred as SNOW plugin or plugin) Configuration and User Guide must be familiar with using the ServiceNow client.

- **Product version**—This document applies to Foundation and CloudScape SNOW plugin v1.0 release.

Information about ServiceNow configuration with Foundation and CloudScape is presented in the following sections:

- ServiceNow Plugin Introduction
- Configuring and Setting Up the Plugin
- RISC SNOW Workflows
- Support and Troubleshooting
- Acronyms

**ServiceNow Plugin Introduction**

The ServiceNow plugin for RISC Networks facilitates to connect to the RISC Platform to perform data sync between ServiceNow and RISC Platform using HTTPS connection.

The primary feature of the plugin is to synchronize the data between ServiceNow and RISC Platform. The plugin is called from the ServiceNow scheduler to fetch data from the RISC Platform. The data updated in ServiceNow Configuration Management Database (CMDB) is updated back to RISC database based on the scheduler configuration.
Overview

The RISC SNOW plugin supports following features:

- Schedule job to import RISC data into SNOW and map it to CMDB
- Discover and list the RISC Platform on the SNOW plugin
- Add tags
- Create CI Relationship of the data that is fetched from RISC Network into CMDB

Prerequisites

Before you begin installation of the plugin, you must have the following resources available:

<table>
<thead>
<tr>
<th>Table 2-17 • Prerequisites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
</tr>
<tr>
<td>ServiceNow</td>
</tr>
<tr>
<td>Web browsers</td>
</tr>
</tbody>
</table>

Prior to using the plugin workflows, the following configurations must be set:

- The xml plugin is imported in ServiceNow
- You have a RISC Networks credential with entitlement to data
- As an end-user, you should be assigned the 'itil and x_riscn_risc_netwo.user[_]' role for viewing or performing any action.

Configuring and Setting Up the Plugin

You must have administrative privileges to configure the plugin. You need to perform the following settings and configurations before you use the plugin:

- Import the XML plugin in ServiceNow
- Configure customer

The steps you need to take to configure and set up the plugin are described in the following topics:

- Importing the Plugin in ServiceNow
- Uninstalling the Plugin
- Creating a User
- Providing Roles to a User
- Connecting to External Systems
- Configuring RISC Networks Credential
- Testing the Configuration
Importing the Plugin in ServiceNow

This section describes the detailed steps to import the `<.xml>` file. You must import the plugin within a specified instance. After the xml file is committed successfully, the project data is available to the users within ServiceNow.

**Task**

To import the plugin:

1. Open the required instance and login using the credentials. You must login using Admin user profile.

2. Type Update Sets in the left pane Search box and click Retrieved Update Sets on the left pane.

3. Click Import Update Set from XML. The Import XML page displays.

4. Click Choose File and click Upload.

   **Note**  • *After the XML file is imported, it displays the status as "Loaded".*

5. Click the uploaded file. In the following screen, click Preview Update Set.
The plugin is successfully committed, you can view the details. Following is a sample screen.

You have successfully imported the plugin.

*Note* • For instructions on how to uninstall the plugin, refer to *Uninstalling the Plugin*.

**Uninstalling the Plugin**

This section describes the steps to delete and uninstall applications from instances.

- Deleting an Application
- Uninstalling an Application

**Deleting an Application**

To delete an application, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To delete applications:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Navigate to the System Application &gt; Applications.</td>
</tr>
</tbody>
</table>
2. In the Develop tab, open the application you want to delete.

3. Click the Delete button on the top-right corner. The Confirmation popup window displays.

4. Click Delete to delete the application. Following confirmation window displays.

5. Enter "delete" in the text box and click OK.

6. For more details to delete an application, see Delete an application in the ServiceNow documentation.
Uninstalling an Application

To uninstall an application, perform the following steps.

**Task**

**To uninstall the application:**

1. Navigate to System Application > Applications.

2. In the Downloads tab, open the Application you want to delete from the list.

3. Click the name or the icon of the installed application to uninstall.

4. Click Uninstall. A confirmation window displays.
5. Click OK.

![Uninstall](image)

6. A confirmation windows displays. Enter "uninstall" and click OK.

![Uninstall](image)

Note • You cannot uninstall applications that are listed under the Develop tab, but you can delete them. Applications downloaded and installed from ServiceNow repository/store can be uninstalled or you can see the “uninstall” related link. For more details to uninstall applications, see ServiceNow.

Creating a User

The administrator needs to create users after importing the plugin for the first time.

Task  To create a user:

1. Open the required instance and login using the credentials.

2. Under the RISC NETWORKS group in the left pane, type users in the navigation pane.
3. Click System Security > Users. Following is a sample screen.

![Sample Screen of Users](image1)

4. Click New to create a new user. The following New record page displays.

![New User Record](image2)

5. Enter the required details and click Submit.

After creating a new user, the administrator needs to provide roles to the user, as described in Providing Roles to a User.

### Providing Roles to a User

To provide roles to a user, perform the following steps.

**Task**

*To provide a role to a user:*

1. Open the required instance and login using the credentials.

2. Under the RISC NETWORKS group in the left pane, type users in the navigation pane.
3. Click System Security > Users. Following is a sample screen.

![Sample Screen of System Security Users](image1)

4. Click on the user whom you want to provide the roles. Following is a sample screen. Scroll the following screen to the bottom.

![User Details](image2)

5. In the Roles tab, click the Edit button.

![Roles Tab](image3)
6. Select the required roles and click the required arrow. Following is a sample screen.

![Sample Screen](image)

7. Click Save.

Note • You must provide the "itil" and "x_riscn_risc_netwo.user" role to the user. Optionally, you can add more roles as required.

Connecting to External Systems

Before you configure the RISC Networks credentials, you must have the UserName, Password, Assessment Code, Host API URL, and API Key.

Configuring RISC Networks Credential

The administrator must have the basic configuration details for the customer configurations such as username, password, assessment code, and host API URL for basic authentication to communicate with the RISC Network database.

Note • Users with the 'x_riscn_risc_netwo.user' role can create and update the customer configuration records.
To configure a customer:

1. Open the required instance and login using the credentials.

2. Under the RISC NETWORKS group in the left pane, click Customer Configurations.

3. Enter the UserName, Password, Assessment Code, Host API URL and API Key.
   The Host API URL is <https://api.riscnetworks.com:443/1_0>.

4. Select the Max. No. of Workers required from the list (values can be 1 to 8).

   Note • If you provide the value as one, import will be slower but other ServiceNow related activities will be optimal. Whereas if you provide the value as 8, multiple threads will execute, and more number of workers (threads) will import data faster into ServiceNow. In this case, other activities will be affected.

5. Click the following as required:

   a. Save Configuration to save the basic configurations.

   b. Sync Data to fetch the RISC Networks data for the configured customer. You are redirected to the Queue page. Refresh the page until the Queue is empty.

   c. Clear All Asset Data to remove the device data. You are redirected to the Queue page. Refresh the page until the Queue is empty.
Testing the Configuration

To test the configuration, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To test the configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the required instance and login using the credentials.</td>
</tr>
<tr>
<td>2.</td>
<td>Under the RISC NETWORKS group in the left pane, click Customer Configurations.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Sync Data. The data between ServiceNow and RISC Platform is synced.</td>
</tr>
</tbody>
</table>

RISC SNOW Workflows

This section provides an overview of the various tasks that you can perform in the plugin.

- Discoverable Devices
- Viewing the SNOW Workflows
- Listing Devices
- Adding Tags
- Viewing the Relationship
- CI Relationship
- Viewing Existing CI and RISC CI Relationship
- Creating Relationship Manually

Discoverable Devices

You can discover the following devices using the RISC SNOW plugin:

- Customer Configurations*
- RISC Basic Devices*
- RISC Cisco CallManagers*
- RISC Inaccessible Devices*
- RISC Inaccessible Network Infrastructure*
Chapter 2  Foundation and CloudScape Overview

How We Collect

- RISC Inaccessible Windows Devices*
- RISC IP Phones*
- RISC Linux and Unix Device*
- RISC Network Infrastructures*
- RISC Virtual Machines*
- RISC VMware Hosts*
- RISC Windows Servers*
- RISC Windows Workstations*
- RISC Queues
- RISC Interfaces
- RISC IPs
- RISC Tags*
- RISC Device and Stacks*
- RISC Stacks*
- RISC Locations
- RISC Storages
- RISC Windows Server Interfaces
- RISC Devices Lifecycles
- RISC Windows Server Disks
- RISC Network Entities
- RISC VMware Host Interfaces
- RISC HBAs
- RISC SCSILUNs
- RISC Stack Relationships
- RISC Device Issues
- RISC Support*
- RISC Logsprt Module

* Asterisk (*) indicates that only these workflows are available to the end-user in the left pane.
Viewing the SNOW Workflows

To view the SNOW workflows, perform the following steps.

Task | To view the SNOW workflows:

1. Login to the ServiceNow portal.
2. In the left panel Search box, type RISC.
3. Click the required link to view more details in the right pane and perform various actions.
Listing Devices

You can view a list of discovered devices available in the RISC Network using the SNOW plugin.

**Task**  
*To list the discovered devices:*

1. Login to the ServiceNow portal.
2. In the left panel Search box, type RISC.
3. Click RISC Basic Devices to view the basic devices. A list of available basic devices is listed in the right pane. Similarly, you can view other devices as well.
4. Click the Device ID to view more details of the device.
5. You can view the Interfaces, IPs, Stacks, Tags, and Location of the device by clicking the respective tabs. The tabs will vary depending on the selected device. For example, for RISC Network, it will additionally list the Network Entity tab and for the RISC Linux and UNIX devices, it lists the Location, Stacks, Tags, Interface and Storage tab.
Adding Tags

Tags allow grouping and organizing of records. You can tag different types of records that are related to the same device. In addition, you can tag devices that you want to work on first. You can add tags, and view your tagged items. You can add tags to the list of discovered devices available in the RISC Network using the SNOW plugin.

**Task**  
**To add tags to the discovered devices:**

1. Login to the ServiceNow portal.
2. In the left panel Search box, type RISC.
3. To add tags to basic devices, click RISC Basic Devices. A list of available basic devices is listed in the right pane.

   **Note** • Select the device to which you want to add tagging.

4. Select the Device ID and click Add RISC Tags.

   **Note** • Alternatively, you can select a Device ID, right-click the device, and then click Add RISC Tags.
A list of existing tags displays as follows.

5. Select the required tag and click Submit Tags.

6. On successfully adding a tag, a success message displays.

After you add the tag, the tag is added to the devices on RISC Network devices. The same is visible in SNOW after the data is synced as per the defined sync schedule in the Tags tab as follows.

Similarly, you can add tags for other devices as well.
Viewing the Relationship

After you synchronize the data, RISC Platform data is imported into ServiceNow and mapping is done to create database relationship by the plugin. The RISC Platform data and their relationship are available in the ServiceNow CMDB table.

The following section describes an example of how you can list the relationship of devices.

Task  To view the relationship of devices:

1. Login to the ServiceNow portal.
2. In the left panel Search box, type RISC.
3. Click RISC Stacks. A list of available RISC Stacks is listed in the right pane.

Note  • Select the device to view the relationship.
4. Click the required StackName to view the relationship.

5. To list the dependency views, click the following button in the Related Items section.

The following is a sample dependency view.
6. To view the dependency in expanded view, right-click the stack and click Expand. Following is a sample screen of the Force view.

7. The arrows indicate the direction of data flow.
8. Scroll down to view the relationship of the selected Stack with other devices. Click the required tab to view the details as follows.

CI Relationship

You can view the relationship between the existing data in SNOW and new data from RISC Networks. In addition, you can manually create the relationship.

Viewing Existing CI and RISC CI Relationship

To create a relationship, search for the existing device in order of preferences of:

- Serial Number
- IP/MAC Address

If a common device is found then both the device will be matched under the 'Identical' Relation Type as shown in the following figure.

Note • If similar device ID is present in two different devices, then you can view the CI relationship of the two devices under the CI Relation tab.

Task

To view CI relationship:

1. Login to the ServiceNow portal.
2. Click on a device.
3. Select the device and click it to open the details page.
Creating Relationship Manually

If you need to create a relationship between the existing data in SNOW and new data from RISC Networks, you can create a relationship as follows in the Relationship Editor.

Figure 2-3: Relationship Editor
**Task**

To create a relationship manually:

1. In the Filter section, enter the required parameters as required. Following is an example.

2. Select an item from the Configuration Items section.

3. Click the plus sign button:

   ![Image](image-url)

   The selected item is added to the Relationships table. Following is a sample screen.

4. Click Save to save the created relationship.
Support and Troubleshooting

Information about support and troubleshooting of a ServiceNow configuration is described in the following topics:

- Viewing Logs
- Setting Log Level
- Service Level Agreement Details
- Troubleshooting and Common Errors

Viewing Logs

You must collect the logs in case you need to contact Flexera Support. Only administrator can view the logs.

Task | To view logs:
--- | ---
1. Login to the ServiceNow portal.
2. In the left panel Search box, type RISC.
3. Click RISC Logs in the left navigation pane. The logs are displayed in the right pane. Following is a sample screen.
4. Click the required log to view more details of a specific log. Following is a specific log detail.
Note • The log levels are displayed depending on the level set by the administrator. For more details, see the Setting Log Level.

Setting Log Level

The administrator can set the log level as follows.

Task To set the log levels:

1. Login to the ServiceNow portal.
2. In the left panel Search box, type sys_properties.list.
3. Type risc in the Name field. A list of <risc<x>.<x>> logs display.
4. Click the x_riscn_risc_netwo.logger.level_ log to set the log level. Following is a sample screen.

5. Enter the level you want to set in the Value field. The Description field describes the log levels. Currently, you can set the following log level as required.
   - 0—Error
   - 1—Error and warning
   - 2—Information, error and warning
   - 3—Debug, information, error and warning
6. Click Update.
Service Level Agreement Details

This section describes the support details that you may need to raise a support request to RISC Networks while using RISC Networks SNOW Plugin.

Table 2-18 • Service Level Agreement Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Hours of Operation</td>
<td>9am - 5pm EST</td>
</tr>
<tr>
<td>Support Days of Operation</td>
<td>Monday - Friday - Except US federal holidays</td>
</tr>
<tr>
<td>Promised Ticket Response Time</td>
<td>1 business day</td>
</tr>
<tr>
<td>Promised Ticket Resolution Time</td>
<td>Not listed</td>
</tr>
<tr>
<td>Contact Method</td>
<td>website, email</td>
</tr>
<tr>
<td>Contact Details</td>
<td><a href="https://portal.riscnetworks.com/">https://portal.riscnetworks.com/</a></td>
</tr>
<tr>
<td></td>
<td>You can contact the Flexera Support team using the Flexera Community.</td>
</tr>
</tbody>
</table>

Note • You must keep the log details handy before you contact the Flexera Support team. For details about viewing logs, see Viewing Logs.

Troubleshooting and Common Errors

This section describes the common errors faced while working with the plugin and solution to resolve them.

Table 2-19 • Common Errors

<table>
<thead>
<tr>
<th>Error</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors with &lt;5xx&gt; code</td>
<td>Report the errors that have &lt;5xx&gt; error code to the Flexera Support team.</td>
</tr>
<tr>
<td>Error with 400 error code</td>
<td>The error is related to plugin. Contact the Flexera Support team.</td>
</tr>
<tr>
<td>Error with 401 error code</td>
<td>Check if the authentication details are correct.</td>
</tr>
<tr>
<td>Error with 429 error code</td>
<td>If the RISC Server receives too many requests at a time, this error displays. Wait for about an hour and retry the operation.</td>
</tr>
</tbody>
</table>

Note • For details about contacting the Flexera Support team, see Service Level Agreement Details.
Acronyms

The following acronyms are used when discussing the ServiceNow plugin:

Table 2-20 • Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB</td>
<td>Configuration Management Database</td>
</tr>
<tr>
<td>SNOW</td>
<td>RISC Networks Service Now</td>
</tr>
</tbody>
</table>

Configuration Items in ServiceNow

The intent of this section is to provide documentation on the usage of the ServiceNow integration and on the data added to ServiceNow through the integration.

The following list details the configuration items created in ServiceNow through the RISC Networks plugin (available through the ServiceNow Store) as well as what data is included with those configuration items.

Included With All Devices

The following configuration items are included with all devices.

Table 2-21 • Configuration Items Included With All Items

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISC Networks Issue Information</td>
<td>Platform checks that were failed by the device:</td>
</tr>
<tr>
<td></td>
<td>● Issue name</td>
</tr>
<tr>
<td></td>
<td>● Problem ID—Unique identifier of this issue.</td>
</tr>
<tr>
<td></td>
<td>● Affected instance—Represents the specific instance that failed the check (such as for a check on disk utilization, 'C:').</td>
</tr>
<tr>
<td></td>
<td>● Issue description</td>
</tr>
<tr>
<td></td>
<td>● Metric—Represents the value that exceeded the threshold of the check (such as for a memory utilization check, this would indicate percent of memory utilized).</td>
</tr>
<tr>
<td></td>
<td>● Issue detail—May provide additional details (such as for overutilized interface, the metric shows discards, this adds utilization for context).</td>
</tr>
<tr>
<td>RISC Networks stack membership</td>
<td>● RISC Networks stack membership</td>
</tr>
<tr>
<td>RISC Networks tags applied</td>
<td>● RISC Networks tags applied</td>
</tr>
<tr>
<td>RISC Networks location</td>
<td>● RISC Networks location</td>
</tr>
<tr>
<td>Licensed</td>
<td>Is the device currently licensed in the Foundation and CloudScape platform?</td>
</tr>
</tbody>
</table>
Table 2-21 • Configuration Items Included With All Items

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>Uniquely identifies the device.</td>
</tr>
</tbody>
</table>

RISC Network Infrastructure

The following configuration items are regarding the RISC network infrastructure.

Table 2-22 • Configuration Items Regarding the RISC Network Infrastructure

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>• Device type—Switch, router, etc</td>
</tr>
<tr>
<td></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Model description</td>
</tr>
<tr>
<td></td>
<td>• Family—Model family</td>
</tr>
<tr>
<td></td>
<td>• Feature set</td>
</tr>
<tr>
<td></td>
<td>• Firmware version</td>
</tr>
<tr>
<td></td>
<td>• Software version</td>
</tr>
<tr>
<td></td>
<td>• Serial number</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Vendor</td>
</tr>
<tr>
<td></td>
<td>• IP/MAC Address—This is the IP that the device was discovered on and what we use for performance polling.</td>
</tr>
<tr>
<td>Interface Information</td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Index</td>
</tr>
<tr>
<td></td>
<td>• ID</td>
</tr>
<tr>
<td></td>
<td>• MAC address</td>
</tr>
<tr>
<td></td>
<td>• Operational status</td>
</tr>
<tr>
<td></td>
<td>• Administrative status</td>
</tr>
<tr>
<td></td>
<td>• Speed</td>
</tr>
<tr>
<td></td>
<td>• Type</td>
</tr>
</tbody>
</table>
### Table 2-22 • Configuration Items Regarding the RISC Network Infrastructure

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Entity Information</strong></td>
<td>Includes information on each component (chassis, line card, etc)</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Firmware version</td>
</tr>
<tr>
<td></td>
<td>• Hardware version</td>
</tr>
<tr>
<td></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Serial</td>
</tr>
<tr>
<td></td>
<td>• Software version</td>
</tr>
<tr>
<td></td>
<td>• class</td>
</tr>
<tr>
<td><strong>Device Lifecycle Information</strong></td>
<td>May include information on different components</td>
</tr>
<tr>
<td></td>
<td>• model</td>
</tr>
<tr>
<td></td>
<td>• description</td>
</tr>
<tr>
<td></td>
<td>• class</td>
</tr>
<tr>
<td></td>
<td>• serial</td>
</tr>
<tr>
<td></td>
<td>• software version</td>
</tr>
<tr>
<td></td>
<td>• lifecycle status</td>
</tr>
<tr>
<td></td>
<td>• lifecycle dates</td>
</tr>
<tr>
<td></td>
<td>• bulletin url</td>
</tr>
<tr>
<td><strong>List of IP addresses</strong></td>
<td>List of IP addresses</td>
</tr>
</tbody>
</table>

### Windows Servers/Workstations

The following configuration items are regarding Windows Servers/Workstations.

### Table 2-23 • Configuration Items Regarding Windows Servers/Workstations

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Information</strong></td>
<td>Device type—Server or workstation. Will include 'Virtual' if it was discovered through VMware as well.</td>
</tr>
<tr>
<td></td>
<td>• Hostname</td>
</tr>
<tr>
<td></td>
<td>• IP/MAC Address—This is the IP that the device was discovered on and what we use for performance polling.</td>
</tr>
<tr>
<td></td>
<td>• Asset—If there is a relationship created between the RISC CI and an existing CI, the asset type of the existing CI will be populated here.</td>
</tr>
</tbody>
</table>
### Table 2-23 • Configuration Items Regarding Windows Servers/Workstations

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Information</td>
<td>Populated only if this device is a VMware guest and VMware credentials were included in discovery</td>
</tr>
<tr>
<td></td>
<td>• ESX Host</td>
</tr>
<tr>
<td></td>
<td>• Power state</td>
</tr>
<tr>
<td></td>
<td>• Tool status</td>
</tr>
<tr>
<td></td>
<td>• UUID</td>
</tr>
<tr>
<td>Operating System Details</td>
<td>• OS</td>
</tr>
<tr>
<td></td>
<td>• Service pack</td>
</tr>
<tr>
<td></td>
<td>• OS version</td>
</tr>
<tr>
<td></td>
<td>• Guest name and Guest OS—Populated only if this device is a VMware guest and VMware credentials were included in discovery.</td>
</tr>
<tr>
<td>Hardware Details</td>
<td>• RAM</td>
</tr>
<tr>
<td></td>
<td>• Serial</td>
</tr>
<tr>
<td></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Vendor</td>
</tr>
<tr>
<td>CPU Details</td>
<td>• CPU speed</td>
</tr>
<tr>
<td></td>
<td>• CPU count</td>
</tr>
<tr>
<td></td>
<td>• CPU model</td>
</tr>
<tr>
<td></td>
<td>• CPU reservation—Populated only if this device is a VMware guest and VMware credentials were included in discovery and a CPU reservation has been set. No value or a value of -1.0 indicates no reservation.</td>
</tr>
<tr>
<td>Hardware Lifecycle</td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• lifecycle dates</td>
</tr>
<tr>
<td></td>
<td>• Bulletin URL</td>
</tr>
<tr>
<td>OS Lifecycle</td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Lifecycle dates</td>
</tr>
<tr>
<td></td>
<td>• Bulletin URL</td>
</tr>
</tbody>
</table>
Linux/Unix Servers

The following configuration items are regarding Linux/Unix servers.

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
</table>
| Interface Information | • Description  
|                   | • Name  
|                   | • Manufacturer  
|                   | • Type  
|                   | • Connection ID  
|                   | • Index  
|                   | • MAC  
|                   | • IP addresses and masks  
|                   | • DHCP details  
|                   | • DNS Details  
|                   | • Default TOS value  |
| Disk Information | • Name  
|                  | • Model  
|                  | • ID  
|                  | • Interface type  
|                  | • Media type  
|                  | • Sector/track/cylinder/head counts  
|                  | • Partition count  
|                  | • SCSI details (port, LU, bus, etc)  
|                  | • Status  
|                  | • Size  |

**Table 2-24 • Configuration Items Regarding Linux/Unix Servers**

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
</table>
| Basic Information | • Host name  
|                   | • Device type—Will include 'Virtual' if it was discovered through VMware as well.  
|                   | • IP/MAC Address—This is the IP that the device was discovered on and what we use for performance polling.  |
### Table 2-24 • Configuration Items Regarding Linux/Unix Servers

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMware Information</strong></td>
<td>Populated only if this device is a VMware guest and VMware credentials were included in discovery</td>
</tr>
<tr>
<td></td>
<td>• ESX Host</td>
</tr>
<tr>
<td></td>
<td>• Power state</td>
</tr>
<tr>
<td></td>
<td>• Tool status</td>
</tr>
<tr>
<td></td>
<td>• UUID</td>
</tr>
<tr>
<td><strong>Operating System Details</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS</td>
</tr>
<tr>
<td></td>
<td>• Distribution</td>
</tr>
<tr>
<td></td>
<td>• OS version</td>
</tr>
<tr>
<td></td>
<td>• Guest name and Guest OS—Populated only if this device is a VMware guest and VMware credentials were included in discovery.</td>
</tr>
<tr>
<td><strong>Hardware Details</strong></td>
<td>• RAM</td>
</tr>
<tr>
<td></td>
<td>• Serial</td>
</tr>
<tr>
<td></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Vendor</td>
</tr>
<tr>
<td><strong>CPU Details</strong></td>
<td>• CPU speed</td>
</tr>
<tr>
<td></td>
<td>• CPU architecture</td>
</tr>
<tr>
<td></td>
<td>• CPU count</td>
</tr>
<tr>
<td></td>
<td>• CPU model</td>
</tr>
<tr>
<td></td>
<td>• CPU reservation—Populated only if this device is a VMware guest and VMware credentials were included in discovery and a CPU reservation has been set. No value or a value of -1.0 indicates no reservation.</td>
</tr>
<tr>
<td><strong>Hardware Lifecycle</strong></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Lifecycle dates</td>
</tr>
<tr>
<td></td>
<td>• Bulletin URL</td>
</tr>
<tr>
<td><strong>OS Lifecycle</strong></td>
<td>• Status</td>
</tr>
<tr>
<td></td>
<td>• Lifecycle dates</td>
</tr>
<tr>
<td></td>
<td>• Bulletin URL</td>
</tr>
</tbody>
</table>
VMware Guests

The following configuration items are regarding VMware Guests.

Table 2-25 • Configuration Items Regarding VMware Guests

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>● Host name</td>
</tr>
<tr>
<td></td>
<td>● ESX Host</td>
</tr>
<tr>
<td></td>
<td>● Device type—Will indicate other collection type if present (ie Virtual-Windows Server).</td>
</tr>
<tr>
<td></td>
<td>● Power state</td>
</tr>
<tr>
<td></td>
<td>● Tools status</td>
</tr>
<tr>
<td></td>
<td>● UUID</td>
</tr>
<tr>
<td>Operating System Details</td>
<td>● OS—Populated if collected via WMI/SSH</td>
</tr>
<tr>
<td></td>
<td>● OS version—Populated if collected via WMI/SSH</td>
</tr>
<tr>
<td></td>
<td>● Guest name and Guest OS</td>
</tr>
<tr>
<td>Hardware Details</td>
<td>● RAM</td>
</tr>
<tr>
<td></td>
<td>● Serial</td>
</tr>
<tr>
<td></td>
<td>● Model</td>
</tr>
<tr>
<td></td>
<td>● Vendor</td>
</tr>
</tbody>
</table>
VMware Hosts

The following configuration items are regarding VMware Hosts.

Table 2-26 • Configuration Items Regarding VMware Hosts

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Information</strong></td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td></td>
</tr>
<tr>
<td>Hardware model</td>
<td></td>
</tr>
<tr>
<td>Vendor</td>
<td></td>
</tr>
<tr>
<td>ESX version</td>
<td></td>
</tr>
<tr>
<td>UUID</td>
<td></td>
</tr>
<tr>
<td><strong>HBA Information</strong></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>PCI address</td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td></td>
</tr>
<tr>
<td>HBA key</td>
<td></td>
</tr>
<tr>
<td>Driver</td>
<td></td>
</tr>
<tr>
<td>Device name</td>
<td></td>
</tr>
<tr>
<td>Bus</td>
<td></td>
</tr>
</tbody>
</table>
Basic Devices
The following configuration items are regarding basic devices.

Table 2-27 • Configuration Items Regarding Basic Devices

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>• Host name</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• Device type</td>
</tr>
</tbody>
</table>
Inaccessible Network Devices

The following configuration items are regarding inaccessible network devices.

Table 2-28 • Configuration Items Regarding Inaccessible Network Devices

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>• Host name</td>
</tr>
<tr>
<td></td>
<td>• Device type</td>
</tr>
<tr>
<td></td>
<td>• Description—From CDP/LLDP neighbor</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
</tbody>
</table>

Inaccessible Windows Devices

The following configuration items are regarding inaccessible Windows devices.

Table 2-29 • Configuration Items Regarding Inaccessible Windows Devices

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>• IP address</td>
</tr>
</tbody>
</table>

IP Phones

The following configuration items are regarding IP phones.

Table 2-30 • Configuration Items Regarding IP Phones

<table>
<thead>
<tr>
<th>Category</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>• Host name</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
</tbody>
</table>

Deployment Requirements

This section explains the deployment requirements for the RN150 Virtual Appliance.

The RN150 is a Debian/GNU Linux Virtual Appliance. It is deployed on VMware ESX or ESXi Server (version 5.5 or later), VMware Player, or VMware Workstation.

- Resource Default Requirements
- Communication Protocols
- Required Credentials and Parameters
Resource Default Requirements

The following the default resource requirements.

Table 2-31 • Resource Default Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8 GB of RAM (minimum 4 GB)</td>
</tr>
<tr>
<td>vCPUs</td>
<td>2 vCPUs (minimum 1 vCPU)</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>50 GB Hard drive (Thin Provisioned)</td>
</tr>
<tr>
<td>Internet access</td>
<td>TCP Port 443 outbound to the following:</td>
</tr>
<tr>
<td>(TCP Port 443)</td>
<td>• orchestration.risncnetworks.com (34.192.184.110, 34.192.195.90)</td>
</tr>
<tr>
<td></td>
<td>• initial.risncnetworks.com (34.192.43.78, 34.192.198.28)</td>
</tr>
<tr>
<td></td>
<td>• dataup.risncnetworks.com (34.192.12.37, 34.192.197.132)</td>
</tr>
<tr>
<td></td>
<td>• app3.risncnetworks.com (34.192.198.73)</td>
</tr>
<tr>
<td></td>
<td>• Backup &amp; Growth (34.192.99.153, 34.192.185.36)</td>
</tr>
<tr>
<td>Internet access</td>
<td>UDP Port 123 outbound to the following:</td>
</tr>
<tr>
<td>(UDP Port 123)</td>
<td>• ntp.risncnetworks.com (3.231.5.12, 18.204.38.15)</td>
</tr>
</tbody>
</table>

Note • If this requirement cannot be met, due to, for example, requiring a proxy, a local NTP server can be specified instead, or NTP can be disabled which will automatically enable ESXi host timesync. See Appliance NTP Support for details.

Communication Protocols

The RN150 uses the following protocols (ports) to access the network. These protocols/ports should be permitted between the RN150 and all local resources (servers, routers, etc) to be included in the discovery.

Table 2-32 • Communication Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>443</td>
<td>RN150</td>
<td>Internet</td>
<td>For communication from the RN150 to the RISC Networks Cloud Orchestration layer</td>
</tr>
<tr>
<td>UDP</td>
<td>123</td>
<td>RN150</td>
<td>Internet</td>
<td>For synchronizing appliance time via NTP</td>
</tr>
<tr>
<td>ICMP</td>
<td>—</td>
<td>RN150</td>
<td>Local Networks</td>
<td>By the RN150 for base discovery for available devices</td>
</tr>
<tr>
<td>TCP</td>
<td>135</td>
<td>RN150</td>
<td>Local Networks</td>
<td>By the RN150 to obtain WMI information from Windows hosts discovered</td>
</tr>
</tbody>
</table>
### Table 2-32 • Communication Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>1024-65535</td>
<td>RN150</td>
<td>Local Networks</td>
<td>RPC Dynamic Port Allocation used for WMI communication.</td>
</tr>
<tr>
<td>TCP</td>
<td>80</td>
<td>RN150</td>
<td>Local Networks</td>
<td>By the RN150 to obtain HTTP</td>
</tr>
<tr>
<td>UDP</td>
<td>161</td>
<td>RN150</td>
<td>Local Networks</td>
<td>Used for gathering SNMP information from devices on the Network</td>
</tr>
<tr>
<td>TCP</td>
<td>443</td>
<td>RN150</td>
<td>Local Networks</td>
<td>Used for gathering VMware guest information directly from vCenter.</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>RN150</td>
<td>Local Networks</td>
<td>By the RN150 to collect from Linux/UNIX servers over the SSH protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>*</td>
<td>RN150</td>
<td>Local Networks</td>
<td>Collection from Linux/UNIX servers via SSH user supplied non-standard TCP ports</td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>RN150</td>
<td>Local Networks</td>
<td>SMB over TCP/IP used for application socket collection</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>RN150</td>
<td>Local Networks</td>
<td>SMB over NetBIOS used for application socket collection</td>
</tr>
<tr>
<td>TCP</td>
<td>8443</td>
<td>RN150</td>
<td>Local Networks</td>
<td>Used for discovering Tomcat and Cisco UC servers*</td>
</tr>
<tr>
<td>TCP</td>
<td>62078</td>
<td>RN150</td>
<td>Local Networks</td>
<td>Used for discovering Apple products (iPhone) – iTunes sync over air port</td>
</tr>
<tr>
<td>TCP</td>
<td>22</td>
<td>RN150</td>
<td>Local Networks</td>
<td>For command line discovery of Cisco Switches and Routers</td>
</tr>
<tr>
<td>TCP</td>
<td>1433**</td>
<td>RN150</td>
<td>Local Networks</td>
<td>For MSSQL database collection only</td>
</tr>
<tr>
<td>TCP</td>
<td>1521**</td>
<td>RN150</td>
<td>Local Networks</td>
<td>For Oracle database collection only</td>
</tr>
<tr>
<td>TCP</td>
<td>3306**</td>
<td>RN150</td>
<td>Local Networks</td>
<td>For MySQL database collection only</td>
</tr>
</tbody>
</table>

**Note** • Double asterisks (**) means that port or other non-standard ports as required for database connectivity.
**Required Credentials and Parameters**

The following are required credentials and parameters:

**Table 2-33 • Required Credentials and Parameters**

<table>
<thead>
<tr>
<th>Credential/Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Subnets           | IP Subnets that the client would like to scan.  
  - These can be added at the time the RN150 is deployed.  
  - Subnets can be manually entered or a routing table can be used to populate the list via SNMP |
| Administrators       | Windows Domain Administrator or Local Administrator (workgroup servers only) credentials.  
  - Needed for WMI access |
| SSH User Account     | SSH user account with sudo privileges  
  - Password or key-based authentication |
| SNMP Read-Only       | Needed for Linux/Unix Servers where not using SSH and should include the following MIBs:  
  - Host-Resources-MIB  
  - UCD-MIB  
  - IF-MIB  
  - TCP-MIB  
  - UCD-DISKIO-MIB  
  - Needed for Network Devices  
  - Supports v1/v2/v3 |
| VMware Credentials   | Read only access to vCenter or root access to ESX hosts directly |
| Database credentials | IP/SIDs of database hosts |

*Note* • For more information, see [SSH Collection Module](#).

*Note* • For more information, see [Database Module](#).
Alternate and Additional Deployment Methods

This section covers deployment methods outside of our typical deployment as well as different types of collection related to our HealthCheck product.

- Appliance Reassociation
- Appliance Proxy Support
- FlexDeploy
- FlexDeploy Getting Started Guide
- Flow Collection (RN50) Deployment Guide
- NAT Configuration for the RN150 Virtual Appliance
- HealthCheck Specific Documentation
- Appliance Certificate Management
- Appliance NTP Support

Appliance Reassociation

Information about appliance reassociation is described in the following topics:

- About Appliance Reassociation
- Prerequisites
- Using Appliance Reassociation
- Appliance Reassociation Troubleshooting

About Appliance Reassociation

The Appliance Reassociation feature allows you to retain a deployed RN150 Virtual Appliance (RN150 VA) and its data when initiating a new assessment. When upgrading from a proof-of-concept to a full subscription, this feature can be utilized to seamlessly begin the full assessment.

Each assessment in the RISC Network platform has an associated RN150 VA. There is a one-to-one association of assessment to RN150 VA deployment. The link between the RN150 VA and the assessment is made once the assessment code is entered into the RN150 VA. The Appliance Reassociation feature allows the user to sever the tie between an existing RN150 VA and an existing running assessment, and re-associate that RN150 VA to a new assessment.
**Data Retained Across Reassociation**

The following data is retained across the reassociation:

- The deployed RN150 VA instance
- Entered subnets
- Entered credentials
- Collected asset data

**Data Not Retained Across Reassociation**

The following data is NOT retained across the reassociation:

- Invited users
- Collected performance data
- CloudScape analytics such as Application Stacks and Move Groups, or HealthCheck reports
- Application of workload licensing to devices

**Prerequisites**

To ensure the confidentiality and integrity of the collected asset data when performing an Appliance Reassociation, these prerequisites are enforced:

- The user initiating the reassociation must be invited to both the original and the new assessments
- The original assessment must be an active, running assessment, having completed at least one discovery scan
- The new assessment cannot have been previously associated with an RN150 VA, or have undergone any configuration activity with the exception of user invitations

If any of these prerequisites are not met, an error message will be displayed when attempting to run the Appliance Reassociation. The error messages are described in the Troubleshooting section below.

**Using Appliance Reassociation**

Utilizing the Appliance Reassociation feature is a straightforward process that begins with provisioning a new assessment instance and instructing the RN150 VA to migrate to that new assessment.

**Provisioning a New Assessment on the RISC Networks Portal**

To provision a new assessment on the RISC Networks Portal, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To provision a new assessment instance on the RISC Networks Portal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the the RISC Networks Portal.</td>
</tr>
<tr>
<td>2.</td>
<td>From the Assessment selection pane, select Add An Assessment</td>
</tr>
<tr>
<td>3.</td>
<td>Enter your subscription code, the name of the assessment, and remaining data</td>
</tr>
</tbody>
</table>
4. Select Submit to create the new assessment instance
5. Access the Appliance Status page by selecting the new assessment from the list
6. Copy to the clipboard or note the assessment code for the new assessment

**Provisioning a New Assessment on the Existing RN150 VA**

To provision a new assessment on the existing RN150 VA, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To provision a new assessment instance on the existing RN150 VA:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the existing RN150 VA</td>
</tr>
<tr>
<td>2.</td>
<td>Navigate to the Assessment section from the Dashboard</td>
</tr>
<tr>
<td>3.</td>
<td>Under the Migrate This Appliance To A New Assessment section, enter the assessment code for the new assessment</td>
</tr>
<tr>
<td>4.</td>
<td>Select the Apply button</td>
</tr>
<tr>
<td>5.</td>
<td>Select Confirm on the confirmation dialog</td>
</tr>
</tbody>
</table>

Once applied, the RN150 VA will be dissociated from the original assessment and associated with the new one. Any configuration or collection activity going forward will occur in the context of the new assessment. A notification to all users invited to original assessment and/or the new assessment will be notified that the reassociation has taken place.

The collected Asset data will be populated in the new assessment instance, which may take several minutes to complete. As normal, an email notification will be sent once this has completed. You will then be able to review the asset data by logging into the assessment in the RISC Networks Portal and viewing the Assets page.

For CloudScape assessments only, workload licensing can be applied to devices at this time to resume performance collection.

**Appliance Reassociation Troubleshooting**

If any of the prerequisites for the Appliance Reassociation feature are not met, one of the following error messages will be displayed. These error messages, their meaning, and the steps to resolve are described here:

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>This appliance is not associated with an assessment</td>
<td>The assessment code for the existing RN150 VA is not a valid assessment code.</td>
<td>Contact the Flexera Support team using the Flexera Community.</td>
</tr>
<tr>
<td>The assessment code for the new assessment is not valid</td>
<td>The code entered for the new assessment was not entered correctly or otherwise does not correspond to an assessment.</td>
<td>Double check that the code was entered correctly. We recommend accessing the RN150 VA application through a web browser, and using copy/paste to enter the code.</td>
</tr>
</tbody>
</table>
### Appliance Proxy Support

The RISC Networks Virtual Appliances require outbound communication from the customer environment to the RISC Networks Secure Cloud Environment (SCE). In cases where all outbound communication from the customer environment is required to pass through a proxy, the Virtual Appliance can be configured with the proxy parameters for this communication.

The feature supports authenticating or non-authenticating HTTPS proxies. Currently, only the Basic authentication method is supported, Windows NTLM authentication is not supported.
In a FlexDeploy deployment the RN150 and FlexDeploy appliances may both be configured to use a proxy for outbound communications to the SCE, however communication between the RN150 and FlexDeploy appliances will not be proxied, and so must not require traversal of the proxy.

SSL/TLS decryption by the proxy is supported if the proxy presents a root or intermediate certificate that is trusted in the global PKI. Custom internal certificate chains are not currently supported.

For more information on appliance proxy support, see:

- Configuring the Virtual Appliances for Proxy Support
- Proxy Configuration Values
- Appliance Proxy Troubleshooting Steps

### Configuring the Virtual Appliances for Proxy Support

When the appliance is first booted up, it will attempt to utilize DHCP to obtain an IP configuration. It will then test communication with the RISC Networks SCE. If DHCP is not available or the communication with the SCE is not successful, the user will be presented with the Interfaces section of the appliance dashboard. This section allows the user to set or modify the IP configuration of the appliance.

Browse to the Interfaces section of the appliance, then select the “Proxy” button. This will open the dialog for setting the proxy parameters. Once the parameters are set, select the “Submit” or "Apply" button to apply the configuration. The dialog can then be closed. To validate the communication with the SCE, the “Refresh” button can be selected, which will perform the communication validation and indicate the results of that test.

If the proxy settings need to be modified, the same steps should be performed. When the Proxy settings dialog is opened, the current proxy configuration will be displayed, and can be modified as necessary. Once the submit button is selected, the updated configuration will be applied, replacing the previous configuration.

If the "Proxy Address" field of the configuration dialog is empty when the form is submitted, the application will interpret this as a request to remove the proxy configuration, disabling proxy support. This can be utilized as an easy method of removing the configuration if the proxy is no longer needed or desired. Please be aware that removing the proxy configuration in an environment where the connection must be proxied may result in the appliance becoming unable to communicate with the RISC Networks SCE. Always be sure to select “Refresh” from the main Interfaces page after applying a change to the proxy to validate that the appliance can properly communicate.

### Proxy Configuration Values

The proxy configuration dialog allows setting the following values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Address</td>
<td>The IP address of the proxy server.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The TCP port on which the proxy server accepts HTTP requests. All communication to the SCE is conducted over HTTPS, however to ensure full support for various proxy server configurations, this value is provided as well.</td>
</tr>
</tbody>
</table>
Appliance Proxy Troubleshooting Steps

If the appliance is unable to communicate with the RISC Networks SCE following the application of a proxy configuration, a support ticket can be opened through the web portal.

When opening a support ticket regarding the proxy feature, please provide the following information:

- Proxy software in use, for example Squid 3.5.22
- Is an authenticating proxy in use, and if so, what type of authentication
- Any error messages shown in the appliance interface following an unsuccessful communication test
- Any relevant information from the proxy software log

FlexDeploy

RISC Networks' offers an optional deployment architecture that allows all customer specific data to be kept onsite or in a location of the customer’s choosing. For example, all data collected by the RN150 Virtual Appliance will remain within the FlexDeploy pod at the customer site or within an environment that the customer chooses to use for data warehousing. The
FlexDeploy architecture from RISC Networks consists of a separate Virtual Appliance, deployed as an OVF that houses both a data warehouse, as well as RISC Networks’ analytics engine. All customer data is processed within the pod and can be accessed by browsing to the local FlexDeploy pod IP address (e.g. https://192.168.1.100).

**Figure 2-4:** Secure Cloud Deployment vs. FlexDeploy

FlexDeploy is described in the following sections:

- FlexDeploy Requirements
- FlexDeploy Pod Internet Access Requirement
- FlexDeploy Technical Architecture
- Customer Responsibilities for FlexDeploy

### FlexDeploy Requirements

A Flex Deploy pod is instantiated by deploying an OVF file into the customer’s VMware infrastructure. RISC Networks FlexDeploy is only supported on VMWare ESXi 5.5 or higher. FlexDeploy pod resource requirements are as follows:

- 4 CPU Cores (vcpus)
- 32 GB of Memory
- 1 TB of Hard Drive
- 1 Network Interface (100Mbps or 1Gbps)

In addition, the FlexDeploy pod server must have outbound Internet access for TCP port 443 to the following:

- **orchestration.riscnetworks.com** (34.192.184.110, 34.192.195.90)
- **initial.riscnetworks.com** (34.192.43.78, 34.192.198.28)
- **app1.riscnetworks.com** (34.192.198.73)
... as well as UDP port 123 to the following if the default NTP server is used:

- ntp-a.riscnetworks.com and ntp-b.riscnetworks.com (3.231.5.12, 18.204.38.15)

**FlexDeploy Pod Internet Access Requirement**

All customer specific data is securely kept on the local FlexDeploy pod (FDP). Only orchestration, authentication, and licensing information is transmitted to the RISC Networks Secure Cloud Environment (SCE). All communication from the FDP to the RISC Networks SCE is handled via SSL Encrypted HTTPS web service calls. No inbound connectivity is required. The FDP uses the secure web service calls to perform the following functions:

- Log users into the appliance and verify their entitlement
- Download security updates and runtime code
- Validate entitlement for device counts and licensing
- Communicate the health of the FDP to the RISC SCE for issue notification
- Synchronize system time
- Facilitate advanced debugging and troubleshooting (requires customer enablement). For more information, see Advanced Debugging.

**FlexDeploy Technical Architecture**

The FlexDeploy pod (FDP) consists of a collapsed storage, analysis, and presentation layer. In RISC Networks cloud based delivery model, these are separate operational units. When run onsite, they are combined into a single entity. All communication between the on-premise RN150 and the on-premise FDP is conducted via HTTPS. Periodically, the RN150 will upload data to the FDP for processing. The upload frequency and size is determined algorithmically to limit impact on the host network. The uploaded data is stored in the FDP until the data processing service is notified and begins to process the data. Processing of the data occurs on the FDP through a number of analytics engines. Once processed, the data is made available in the FlexDeploy database, which is accessible through the FDP web interface. At no time does any customer specific environment data leave the FlexDeploy pod.

**Customer Responsibilities for FlexDeploy**

Because RISC Networks does not have access to the FlexDeploy pod (FDP), we are unable to verify and validate that the underlying VMware infrastructure is properly configured. The customer is responsible for ensuring that the VMware host has adequate CPU/Memory/Disk resources and that the FDP is properly backed up and available for access. Customers who do not wish to handle this responsibility should consider using RISC Networks’ secure cloud based delivery.

In addition, while RISC Networks has implemented technical controls to restrict the leakage of data from the FDP out of the customer environment, RISC Networks can not control access to the FDP itself. The restriction of access to the pod itself is the responsibility of the customer. The destruction of the FDP is also the responsibility of the customer should they choose to stop using the Foundation and CloudScape platform. RISC Networks is not responsible for the following data leakage events/challenges:

- Restricting physical or logical access to the FlexDeploy pod
- Data Exported from the system via the web interface of the FlexDeploy pod
- Failure to properly destroy the FlexDeploy pod VM at the conclusion of use of the Foundation and CloudScape platform
FlexDeploy Getting Started Guide

The following sections describe how to get started using FlexDeploy:

- **Requirements**
- **Assessment Creation**
- **Getting the Appliance**
- **Accessing the FlexDeploy**
- **Initial Configuration**
- **RN150 Configuration**

**Requirements**

The requirements for the RN150 will remain the same as with our standard SaaS based deployment option. Please refer to the Deployment Requirements for the most current requirements for RN150 deployment and support.

The requirements for the FlexDeploy option are in addition to the RN150 requirements. Please refer to FlexDeploy for the most current requirements for FDP deployment and support.

**Assessment Creation**

To create an assessment, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To create an assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to portal.riscnetworks.com.</td>
</tr>
<tr>
<td>2.</td>
<td>Create the assessment as normal</td>
</tr>
</tbody>
</table>

Once the RN150 configuration has been completed, the assessment will transition onto your FlexDeploy interface and will only be viewable there.

**Getting the Appliance**

To get the appliance, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To get the appliance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to the Appliance Status page in the portal to access the download link and bootstrap code for the FlexDeploy virtual appliance. The Pod Key will be entered into the FlexDeploy during the deployment process.</td>
</tr>
<tr>
<td>2.</td>
<td>Download the FlexDeploy virtual appliance</td>
</tr>
</tbody>
</table>

This downloads as a ZIP file containing the appliance OVF template files. This is the same process as the RN150 and RN50 appliances.
3. Deploy the FlexDeploy into your VMware vSphere environment

Follow VMware documented procedures for Deploying OVF Templates. This is the same process as the RN150 and RN50 appliances.

The OVF that the appliance is deployed with will automatically configure the virtual machine instance with the recommended hardware configuration.

4. Power on the FlexDeploy appliance

Accessing the FlexDeploy

The FlexDeploy appliance has two user interfaces:

- **Initial configuration interface**—The initial configuration interface is accessible via the VMware console, or by browsing to the virtual appliance IP address over HTTP on TCP port 8000. Once the initial configuration steps are complete, you will not need to revisit the configuration interface.

- **Standard interface**—The standard interface is accessible by browsing to the appliance IP address using HTTP on TCP port 80, or using HTTPS on standard TCP port 443. This will be the same interface you are familiar with on portal.riscnetworks.com. You will be able to access your assessment and reports as normal from this interface. If you browse to this interface prior to performing the initial configuration steps, you will receive a page with a link to redirect you to the initial configuration interface.

Initial Configuration

To perform initial configuration of FlexDeploy, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To perform initial configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure the network interface.</td>
</tr>
<tr>
<td></td>
<td>The FlexDeploy appliance will automatically attempt DHCP. If no DHCP lease is received, you will be automatically redirected to the network configuration page:</td>
</tr>
<tr>
<td></td>
<td>a. Enter a static IP configuration, or troubleshoot DHCP and reattempt.</td>
</tr>
<tr>
<td></td>
<td>b. Enter proxy configuration settings (if applicable).</td>
</tr>
<tr>
<td></td>
<td>If a DHCP lease is received, you will be presented with the login page. You can apply a static configuration later if desired.</td>
</tr>
<tr>
<td>2.</td>
<td>Read and accept the EULA, log in</td>
</tr>
<tr>
<td>3.</td>
<td>Enter the Pod Key. The FlexDeploy appliance will now bootstrap itself, which may take several minutes</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the network interface if desired</td>
</tr>
</tbody>
</table>

**Note** • If a DHCP lease was received previously and you would like to transition to a static address, you will now be able to enter the Interfaces section to set the static IP configuration and proxy settings (if applicable)

5. You have now completed the initial configuration. You can now view the main portal interface by browsing to the FlexDeploy appliance IP address via HTTP or HTTPS.
**RN150 Configuration**

To perform RN150 configuration, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To perform RN150 configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Download the RN150 virtual appliance and obtain the bootstrap code from the Appliance Status page in the portal.</td>
</tr>
<tr>
<td>2.</td>
<td>Deploy as normal.</td>
</tr>
<tr>
<td>3.</td>
<td>Read and accept the EULA, log in.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter the Assessment Code.</td>
</tr>
<tr>
<td>5.</td>
<td>Select to use FlexDeploy. You will be prompted as to whether to deploy on FlexDeploy. Select <strong>Yes</strong>.</td>
</tr>
<tr>
<td>6.</td>
<td>Enter the FlexDeploy appliance IP address. This will associate your RN150 and your assessment to the FlexDeploy appliance. The assessment will now transition onto your FlexDeploy appliance, and will only be viewable from the FlexDeploy interface.</td>
</tr>
<tr>
<td>7.</td>
<td>Continue RN150 configuration as normal.</td>
</tr>
<tr>
<td>8.</td>
<td>Start your assessment.</td>
</tr>
</tbody>
</table>

**Flow Collection (RN50) Deployment Guide**

The following sections describe deployment of Flow Collection (RN50):

- Requirements for Integrating Flow Data into the Foundation and CloudScape Platform
- Overview of Deploying Virtual RN50 Appliances
- VMware Traffic Collection
- Configuring the vSphere Virtual Switch (vSwitch) for Promiscuous Mode Capture
- Collecting Traffic from a Single VLAN Port Group
- vSphere vSwitch Traffic Collection from Multiple VLANs Where Untagged Traffic is Permitted in the Environment
- vSphere vSwitch Traffic Collection from Multiple VLANs Where Untagged Traffic is NOT Allowed in the Environment
- Enable the RN50 Virtual Appliance Virtual Network Interfaces
- vSphere DVS Port Mirroring Configuration
- SPAN Configuration
- Configure Virtual RN50 for SPAN Collection on VMware Workstation
- NetFlow Version 5 Configuration
- Verifying TrafficWatch Collection
Requirements for Integrating Flow Data into the Foundation and CloudScape Platform

Integrating Flow Data into the Foundation and CloudScape platform refers to the use of either Packet Capture or Netflow data streams in order to provide additional information to the standard connectivity reporting. Specifically, this provides data rate information such as Total Bytes, Max Kbps, and Average Kbps that cannot be derived from socket based dependency data alone.

In order to incorporate Flow Data in the Foundation and CloudScape platform an addition appliance (RN50) is required and must be deployed as needed to provide “visibility” into the interesting traffic. The specific deployment scenarios will vary based on the environment and specific requirements. The most common deployment scenarios are discussed below. The key take away is that you must ensure you are providing visibility into all possible network data paths associated with application, and subsequently the specific workloads you are interested in. Capturing most or some of the traffic associated with the applications being measured can lead to inaccurate assumptions.

- Virtual Machines
- Physical Servers
- Netflow

Virtual Machines

For VMware based virtual environments you must deploy the RN50 onto each VMware host (ESXi Hypervisor) that supports the Virtual Machines in-scope for analysis. This is because traffic between two Virtual Machines residing on the same host stays local to the host and does not “hit the wire”. The specific deployment process will depend on the virtual networking deployment in use (i.e. Standard vSwitch or Distributed vSwitch). In this deployment scenario, the RN50 is deployed in packet capture mode (i.e. mirror) using either promiscuous mode (Standard vSwitch) or Port Mirroring (Distributed vSwitch).

Physical Servers

For physical servers (i.e. Windows, Linux, Unix) you must use SPAN or Port Mirroring at the physical switch layer to mirror all interesting traffic to the RN50. In this deployment scenario, the RN50 is deployed in packet capture mode and must be connected to the destination port of the switch SPAN session. It is likely that multiple RN50 appliances will be required depending on the number of physical workloads in scope and their physical connectivity to the switching infrastructure. Keep in mind that the RN50 is a Virtual Appliance and must be deployed on a supported hypervisor with adequate physical resources.

Netflow

If the supporting network infrastructure supports Netflow you can configure the network devices to export Netflow data to the RN50. In this deployment scenario, the RN50 can be deployed in a more centralized fashion and accept data from multiple Netflow sources. Some network devices can only provide Netflow sampling as traffic passes Layer 3 boundaries. In this case, server to server connectivity within the same VLAN would not be visible in the Netflow export. Please consult with your network device manufacture for details on Netflow support and configuration requirements. We recommend limiting the number of Netflow sources reporting to a single RN50 to 20 (10 for busy environments); if you have many Netflow sources multiple RN50s may be deployed for a single assessment.
Overview of Deploying Virtual RN50 Appliances

This document will provide step-by-step instructions on deploying the Virtual RN50 appliances for use in traffic collection including VMware vSphere Virtual Switch Promiscuous mode, Distributed Virtual Switch Port Mirroring, SPAN (Port Mirroring), and NetFlow. Instructions for netstat collection are also included. The specific configuration depends on conditions in the environment, and we will cover the individual steps involved for each use-case. The possible use-cases are detailed below.

- Promiscuous-Mode Mirroring
- VDS Port Mirroring
- SPAN (Switched Port Analyzer)
- Application Socket Collection
- Netflow

Promiscuous-Mode Mirroring

Promiscuous-mode mirroring will expose inter-VM traffic on a VMware virtual switch PortGroup for collection by the RN50 virtual appliance. It is similar to using Port Mirroring on a physical switch to collect mirrored traffic using SPAN, yet is specific to the VMware virtual switch. Traffic flowing through the virtual switch will be mirrored, and captured by the RN50 virtual appliance.

VDS Port Mirroring

VDS Port Mirroring will expose inter-VM traffic on a VMware distributed virtual switch (dvSwitch) for collection by the RN50 virtual appliance. Traffic flowing through the VDS will be mirrored, and captured by the RN50 virtual appliance.

SPAN (Switched Port Analyzer)

SPAN (Switched Port Analyzer) copies traffic from one or more ports, one or more EtherChannels, or one or more VLANs and sends the copied traffic for analysis to the Virtual RN50 virtual appliance.

Application Socket Collection

Netstat is a utility for reporting statistics from the operating system network stack. This utility has been implemented for virtually every major operating system, including Microsoft Windows NT, GNU/Linux, Apple OS X, BSD, and Oracle/Sun Solaris. Most implementations can report on a wide range of statistics, but the most common use of the utility is to provide a list of listening ports or active connections.

Netflow

NetFlow is a protocol designed for network monitoring. It aggregates traffic statistics based on layer 3 and layer 4 flow information in order to determine the top talkers in the environment, and to describe the various protocols and interactions taking place. Devices with NetFlow enabled will gather and record flow statistics and periodically push this data to the RN50. Because NetFlow data is aggregated, and does not include packet contents, the relative volume of data is small.
VMware Traffic Collection

Deploying TrafficWatch will require a standard assessment using the RN150 virtual appliance. An existing, running, assessment can be used, or a new assessment can be created. TrafficWatch will require the RN150 appliance for command-and-control, as well as for data uploads to the RISC Networks NOC for final report generation (FlexPod assessment data will remain onsite). The RN50 appliance is used to collect mirrored traffic from the virtual switch, so an RN50 appliance will need to be deployed on each ESX/vSphere host, or one appliance per virtual switch. The RN50 appliances will require connectivity with the RN150 appliance.

**Important** • *Enabling Promiscuous Mode on a VSS (depending on configuration) will expose all guest VM traffic on that vSwitch and can be considered a security risk. Please consult your VMware administrator for policies regarding exposing server traffic.*

If VLANs are in use in the environment, additional steps may be required. The VMware vSwitch or VDS port groups must be configured appropriately in order to collect mirrored traffic from VLANs. There are four use-cases:

1. VLANs are not in use in the environment
2. VLANs are in use, but traffic is only collected from one particular VLAN
3. VLANs are in use, and untagged traffic is permitted in the environment
4. VLANs are in use, and untagged traffic is NOT permitted in the environment

Details on configuration for each use-case are provided below. The specific steps involved are different depending on whether the classic vSwitch or the Distributed Virtual Switch (VDS) is in use. The step-by-step instructions to follow are broken up into two sections depending on which VMware switching technology is in use. In any case, the initial deployment steps are the same.

- **Downloading the RN50**
- **Deploying the RN50 Virtual Appliance**
Downloading the RN50

To download the RN50, perform the following steps:

1. Browse to the web portal at https://portal.riscnetworks.com/login.php and log in:

   ![Member Login](image1)

   - Email
   - Password
   - Remember Me

   Login

   Forgot Password? | Register

2. Access the assessment by selecting the assessment name.
3. Select Collect Data menu > select Flow / Dependency Data

4. Select Download RN50 Appliance.

Deploying the RN50 Virtual Appliance

To deploy the RN50 virtual appliance, perform the following steps.

Task  To deploy the RN50 virtual appliance:

1. Connect to the ESX host or vCenter via the vSphere Client
2. In the vSphere client, select File, then Deploy OVF Template

3. Browse to the location of the unzipped RN50 download

4. Select the MyIT-RN50-Virtual-Appliance2.0.ovf file

5. Continue to deploy the virtual appliance according to local standards
   - The RN50 OVF defines the basic requirements of the appliance
     - 2GB disk allocation (thick or thin provisioned)
     - 2GB memory allocation
   - Accepting the defaults is recommended

6. Select the appropriate Destination Network
7. Select Finish to finish the deployment
8. Power on the appliance
9. Access the appliance via the VMware console
10. Continue with DHCP or set a static IP configuration by selecting Edit in the Interfaces section.
11. Access the RN150 section

12. Select TrafficWatch from the drop-down list and select Proceed
13. Select Proceed

14. Enter the IP address of the RN150 appliance and select Add
15. Test the connection

16. The RN50 appliance is now ready to collect NetFlow/ESX traffic/Port Mirroring.
Configuring the vSphere Virtual Switch (vSwitch) for Promiscuous Mode Capture

**Use-Case:** No VLANs in use

Promiscuous mode can be configured on the vSwitch PortGroup, or VMKernel. Configuring promiscuous mode on the vSwitch allows all portgroups to see other VM traffic. Configuring promiscuous mode on the portgroup only allows VMs in that portgroup to see other VM traffic on the vSwitch.

---

**Important** • Enabling Promiscuous Mode on a VSS (depending on configuration) will expose all guest VM traffic on that vSwitch and can be considered a security risk. Please consult your VMware administrator for policies regarding exposing server traffic.

Each vSwitch PortGroup defaults to a VLAN ID of 0, (traffic is not tagged). The RN50 virtual appliance will be able to collect traffic from any VM connected to a Port Group set with a VLAN ID of 0. The vSwitch PortGroup must be configured for Promiscuous-Mode. The steps to do so are as follows:

To configure the vSphere Virtual Switch, perform the following steps.

---

**Task**

To configure the vSphere virtual switch:

1. In the vSphere client, Select the ESX host.

---
2. Select the Configuration tab.

3. Select the Networking link under Hardware.
4. Select vSphere Standard Switch.

5. Select the Properties link.

The vSwitch configuration page should now be visible.

6. Select the vSwitch PortGroup the virtual appliance is assigned to.
7. Select Edit.

8. Select the Security tab.

9. Check the box next to Promiscuous Mode

10. Select Accept on the Promiscuous Mode drop-down list
11. Select OK.

Collecting Traffic from a Single VLAN Port Group

If VLANs are in use but the RN50 appliance is only intended to collect traffic from VMs on one particular VLAN, then the RN50 appliance needs to be connected to the Port Group that is configured for that VLAN.

Task To collect traffic from a single VLAN port group:

1. In the list of guest Virtual Machines select and right click the RN50 virtual appliance.
2. Select Edit Settings.

3. Select Network Adapter.
4. In the Network Connection section, select the Port Group associated with the appropriate VLAN.

![Configuration Screen](image)

5. Select OK.

### vSphere vSwitch Traffic Collection from Multiple VLANs Where Untagged Traffic is Permitted in the Environment

If VLANs are in use in the environment and the RN50 appliance is intended to collect traffic from all VLANs, the appliance must be configured to connect through a Port Group set to VLAN ID 4095. This is a VMware-specific VLAN ID that is untagged, yet allows for communication with VMs on all VLANs within the vSwitch. If a PortGroup configured for VLAN ID 4095 already exists, then a new Port Group need not be created.

The steps for configuration are as follows:

<table>
<thead>
<tr>
<th>Task</th>
<th>To configure vSphere vSwitch traffic collection from multiple VLANs (untagged traffic is permitted):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Access the vSwitch Networking Properties.</td>
</tr>
<tr>
<td>2.</td>
<td>In the vSphere client, Select the ESX host.</td>
</tr>
</tbody>
</table>
3. Select the Configuration tab.

4. Select the Networking link under Hardware.
5. Select vSphere Standard Switch.

6. Select the Properties link.
7. Select Add.


9. Define Network Label (Name the PortGroup)
10. Enter 4095 in the VLAN ID section.

![Add Network Wizard](image)

11. Select Next.

12. Select Finish.

13. Return to vSwitch properties.

14. Highlight the 4095 PortGroup.

15. Select Edit.
16. Select the Security Tab.
17. Place a check mark next to Promiscuous Mode: and ensure Accept is selected in the dropdown menu.

![Traffic Collection Policy Exceptions](image)

18. Select OK.

19. Select Close.

vSphere vSwitch Traffic Collection from Multiple VLANs Where Untagged Traffic is NOT Allowed in the Environment

If VLANs are in use and the RN50 appliance is intended to collect traffic from all VLANs, yet untagged traffic is not permitted in the environment, extra configuration is necessary. First, the appliance needs to be configured to connect through a Port Group set to VLAN ID 4095. This is a VMware-specific VLAN ID that is untagged, yet allows for communication with VMs on all VLANs within the vSwitch. In this configuration the RN50 appliance will not be able to communicate across the environment with the RN150 appliance, so an additional interface must be created and configured on the RN50 appliance. If a Port Group configured for VLAN ID 4095 already exists, a new Port Group need not be created.

The steps for configuration are as follows:

<table>
<thead>
<tr>
<th>Task</th>
<th>To configure vSphere vSwitch traffic collection from multiple VLANs (untagged traffic not permitted):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create VLAN PortGroup 4095</td>
</tr>
<tr>
<td>2.</td>
<td>Access the vSwitch Networking Properties</td>
</tr>
</tbody>
</table>
3. In the vSphere client, Select the ESX host.

4. Select the Configuration tab.
5. Select the Networking link under Hardware

6. Select vSphere Standard Switch
7. Select the Properties link.

8. Select Add.

10. Select Next

11. Define Network Label.

12. Enter 4095 in the VLAN ID section.

13. Select Next

14. Select Finish

15. Return to vSwitch properties

16. Highlight the 4095 PortGroup
17. Select Edit.

18. Select the 'Security' Tab.
19. Place a check mark next to Promiscuous Mode: and ensure Accept is selected in the dropdown menu.

20. Select OK.


Enable the RN50 Virtual Appliance Virtual Network Interfaces

To enable the RN50 virtual appliance virtual network interfaces, follow the instructions in Configure Interface 1 and Configure Interface 2.

Configure Interface 1

To configure interface 1, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To Configure Interface 1:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the list of guest Virtual Machines select and right click the RN50 virtual appliance.</td>
</tr>
</tbody>
</table>
2. Select Edit Settings

3. Select Network Adapter 1
4. In the Network Connection section, select the VLAN 4095 Port Group

5. Select OK.

**Configure Interface 2**

To configure interface 2, perform the following steps.

**Task**

To configure interface 2:

1. In the list of guest Virtual Machines select and right click the RN50 virtual appliance.
2. Select Edit Settings

3. Select Network Adapter 2
4. In the Network Connection section, select the Port Group with access to the RN150 virtual appliance.

5. Select OK.

vSphere DVS Port Mirroring Configuration

An RN50 virtual appliance will need to be deployed on each ESX host you wish to collect guest VM traffic.

The steps for configuration are as follows:

**Task**

*To configure vSphere DVS port mirroring:*

1. Access vSphere Client
2. Select Home
3. Select Networking
4. Select the Ports tab

5. Record and save the Port ID numbers for each VM that you wish to include for collection
6. Record and save the Port ID numbers for each RN50 virtual appliance deployed.
7. Right select the dvSwitch and select Edit Settings.

8. Select the Port Mirroring tab
9. Select Add.

10. Supply the Port Mirroring Session Name and Description.

11. Select Allow normal IO on destination ports.
12. Select Next.

13. Enter the Source Port IDs (Port IDs recorded in step 5)

14. Add the Source Port IDs by selecting >>

15. Enter the Destination Port IDs (Port IDs recorded in step 6)
16. Add the Source Port IDs by selecting >>

17. Enable Port Mirroring

19. Verify Port Mirroring Session.

**SPAN Configuration**

*Note* • SPAN configuration may vary depending on the device. Please consult your manufacturer’s documentation for further information regarding port mirroring support for your device.

To perform SPAN configuration, perform the following steps.

**Task**  
To perform SPAN configuration:

1. Switch# configure terminal (Enter global configuration mode.)
2. Switch(config)# monitor session session_number source interface interface-id [, | -] [both | rx | tx]
   - Specify the SPAN session and the source port (monitored port).
   - For session_number, specify 1.
   - For interface-id, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (port-channel port-channel-number).
   - (Optional) [, | -] Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.
• (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.
  • both—Monitor both received and sent traffic.
  • rx—Monitor received traffic.
  • tx—Monitor sent traffic.

3. `Switch(config)# monitor session session_number destination interface interface-id [encapsulation {dot1q}]`
   • Specify the SPAN session and the destination port (monitoring port).
   • For session_number, specify 1.
   • For interface-id, specify the destination port. Valid interfaces include physical interfaces.
   • (Optional) Specify the encapsulation header for outgoing packets. If not specified, packets are sent in native form.
     • dot1q—Use 802.1Q encapsulation.

4. `Switch(config)# end` (Return to privileged EXEC mode)

5. `Switch# show monitor [session_number]` (Verify your entries)

6. `Switch# copy running-config startup-config` (Optional, save your entries in the configuration file.)

---

**Configure Virtual RN50 for SPAN Collection on VMware Workstation**

A virtual RN50 appliance will need to have 2 vNICs configured, 1 vNIC bridged to the Network and 1 vNIC bridged to the SPAN port. Configuration may vary depending the host machine and current VMnet settings on VMware Workstation.

To configure Virtual RN50 for SPAN collection on VMware Workstation, perform the following steps.

| Task |
| To configure Virtual RN50 for SPAN collection on VMware Workstation: |

1. Open VMware Workstation
2. Select Edit
3. Select Virtual Network Editor
4. Highlight VMnet 0
5. Ensure VMnet Information is set to Bridged
6. Set Bridged to: NIC connected to SPAN port on physical switch

7. Select Add Network (VMware Workstation will populate next available VMnet)

8. Select OK

9. Highlight created VMnet

10. Change VMnet Information to Bridged
11. Set Bridged to: NIC with network access (RN50 appliance must have network access to the RN150 appliance)/

12. Select Apply

13. Select OK

14. Select Open Virtual Machine

15. Browse to RN50 folder and select the OVF file

16. Select Open

17. Name Virtual Appliance (Optional)

18. Select Import

19. Select Edit Virtual Machine Settings

20. Highlight Network Adapter

21. Select Custom in the Network Collection field

22. Select the VMnet in the dropdown box assigned to the NIC connected to the SPAN port of physical switch.

23. Select Add
24. Select Network Adapter
25. Select Next
26. Select Custom in the Network Collection field
27. Select the VMnet in the dropdown box assigned to the NIC that has network access to the RN150

![Image of Network Adapter Type]

28. Select Finish
29. Select OK
30. Power on VM.

Successful SPAN configuration will result in the IP address of the RN50 displayed as Mirrored for Collection Type in the TrafficWatch Stats in the RISC portal

**NetFlow Version 5 Configuration**

Cisco includes NetFlow version 5 support on many devices. Please refer to the documentation for your specific devices to determine if they support NetFlow.

NetFlow can be a powerful tool in a RISC Networks TrafficWatch engagement. When deploying NetFlow for TrafficWatch, the RN50 virtual appliance is configured as the NetFlow collector, and each exporter, the infrastructure device reporting NetFlow statistics, counts as a node towards the available node entitlement.

**Quick Setup**

To set up NetFlow Version 5, perform the following steps:

<table>
<thead>
<tr>
<th>Task</th>
<th>To set up NetFlow Version 5:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Deploy RN150 as normal and start assessment.</td>
</tr>
<tr>
<td>2.</td>
<td>Download and deploy RN50.</td>
</tr>
<tr>
<td>3.</td>
<td>Select TrafficWatch.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter IP address of RN150.</td>
</tr>
<tr>
<td>5.</td>
<td>Access devices that will export NetFlow.</td>
</tr>
</tbody>
</table>

7. Configure NetFlow to export to the IP address of the RN50, port 9996.

8. Verify configuration in the portal.


**Configure Device for NetFlow**

To configure a device for NetFlow, specify the following:

- Generic Cisco IOS commands (may vary depending on device):
  
  - Router# configure terminal
  
  - Router(config)# ip cef
  
  - Router(config)# interface <interface> #For each participating interface
  
  - Router(config-if)# ip route-cache flow #For each participating interface
  
  - Router(config-if)# exit
  
  - Router(config)# ip flow-export version 5
  
  - Router(config)# ip flow-export destination <RN50 IP address> 9996
  
  - Router(config)# end
  
  - Verify collection of NetFlow statistics
  
  - Router# show ip flow export
  
  - Router# show ip cache [verbose] flow #Summarizes active flows, indicates how much NetFlow data is being exported
Verifying TrafficWatch Collection

To verify TrafficWatch collection, perform the following steps.

**Task**  
**To verify TrafficWatch collection:**


2. Access the assessment by selecting the assessment name.

3. Select Collect Data menu.

5. Verify each RN50 is associated to the assessment and Online.

6. Verify traffic is being recorded by each RN50 in the Flow Statistics section.

7. The Collection Type column will list the type of capture:
   - NetFlow will display the IP address of the NetFlow exporting device
   - Mirror capture indicates SPAN (port mirroring), Promiscuous Mode Capture (VSS Mirror), or DVS Port Mirroring
8. Current collection can be verified in the Last Record Time (Record times will update on 10 minute intervals)

<table>
<thead>
<tr>
<th>Last Record Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-31-16 15:05 UTC</td>
</tr>
<tr>
<td>10-31-16 15:05 UTC</td>
</tr>
<tr>
<td>10-31-16 15:05 UTC</td>
</tr>
<tr>
<td>10-31-16 15:00 UTC</td>
</tr>
<tr>
<td>10-31-16 15:05 UTC</td>
</tr>
<tr>
<td>10-31-16 15:05 UTC</td>
</tr>
</tbody>
</table>

*Note: If additional assistance is needed, contact the Flexera Support team using the Flexera Community.*

**NAT Configuration for the RN150 Virtual Appliance**

If your SNMP access is restricted to certain IP addresses, and you have a server that is included in that access (i.e. a physical server running existing monitoring software), you can run the appliance in VMware player or VMware Workstation on that server with NAT configuration so it will be seen as accessing the appliance through that host.

Setting the virtual appliance to use NAT with VMware Player & VMware Workstation can be done in the following ways:

- VMware Workstation
- VMware Player

**VMware Workstation**

To perform NAT configuration for the RN150 virtual appliance on VMware Workstation, perform the following steps.

**Task**

To perform NAT configuration for the RN150 virtual appliance on VMware Workstation:

1. Edit virtual machine settings
2. Highlight Network Adapter
3. Select ‘NAT: Used to share the host’s IP address’
4. Select OK
5. Power on the Virtual Appliance
VMware Player

To perform NAT configuration for the RN150 virtual appliance on VMware Player, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To perform NAT configuration for the RN150 virtual appliance on VMware Player:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Player</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td>Select <strong>Manage</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Select <strong>Virtual Machine Settings</strong>…</td>
</tr>
<tr>
<td>4.</td>
<td>Select <strong>Network Adapter</strong>.</td>
</tr>
<tr>
<td>5.</td>
<td>Select <strong>NAT: Used to share the host's IP address</strong>.</td>
</tr>
<tr>
<td>6.</td>
<td>Select <strong>OK</strong>.</td>
</tr>
<tr>
<td>7.</td>
<td>Play the Virtual Appliance.</td>
</tr>
</tbody>
</table>

HealthCheck Specific Documentation

For information on HealthCheck, see the following sections:

- HealthCheck Features
- Traffic Sim Instructions Setup
- TrafficSim Codecs

HealthCheck Features

RISC Networks HealthCheck has some features that are not applicable to the rest of the Foundation and CloudScape platform. The following sections cover those features or description accordingly:

TrafficSim

RISC Networks' TrafficSim engagements require the use of RISC Networks' virtual appliance to simulate and evaluate the performance of real time traffic on the network. Virtual (or physical) RN50 appliances must be deployed and register with the RN150 appliance. These RN50 end points operate as the termination points of a simulation.

CISCO Unified Communications

The Cisco Unified Communications Analytics engagement requires a Unified Communications Manager AXL username and password. Although this username and password combination can be a user within the 'Super Users Group' only 'AXL API Access Group' is required for CUCM 5.X and later. It is recommended to setup a temporary AXL user where possible which then can be deleted at the completion of the Analytics engagement.

Cisco Unified Communications credentials entered on the appliance web interface are encrypted and handled in the same manner as Windows and SNMP credentials. All are maintained on the virtual appliance for the duration of the assessment and until the virtual appliance is deleted.
Traffic Analytics

RISC Networks’ Traffic Analytics module is used to capture actual network traffic and report on traffic profiles within the network. The two methods of deploying traffic analytics, embedded and virtual appliance based.

Embedded Traffic Analytics involves the deployment of Cisco NetFlow within a Cisco environment. This deployment is done via SNMP Write strings which are required in order to deploy embedded Traffic Analytics. RISC Networks does not support user deployed NetFlow configurations. Cisco NetFlow technology provides accounting records only for traffic. No user traffic is captured. Only a record of the traffic (source and destination IP, source and destination port, protocol, bytes, duration, etc) is available.

Virtual appliances capture traffic through a span port on a switch. The virtual appliance does not record any user payload information for use in its analysis. Deep packet analysis that is required is done on the virtual appliance itself as part of a protocol decoder and is used only for statistical analysis. For example an HTTP GET followed by an HTTP 200 OK message would represent the duration of a web site download. This level of analysis may be performed by the virtual appliance but the details of the web page itself, including user input data or return data, are not reported to the virtual appliance for processing. The raw captures of the details are overwritten every 5 minutes on the virtual appliance and are permanently lost after power cycling the virtual appliance.

Data Center Analytics

Data Center Analytics are included in your IT HealthCheck assessment. These add VMware inventory and performance data as well as Fibre Channel inventory and performance data as additional data sets. For VMware, RISC Networks utilizes the VMware published vSphere API in order to collect information from vCenter and individual ESX servers. For ESX servers, the root password is normally required to access the vSphere API. Access to the vSphere API can be tested by pointing a web browser to: https://x.x.x.x/mob

This URL will return a login prompt that will verify the credentials required to access the vSphere API. RISC Networks does NOT use root credentials to log onto ESX or vCenter servers. The API is the only access that RISC Networks has to the VMware environment.

SNMP is used to collect information from Fibre Channel switches. RISC Networks does NOT directly access the Fibre Channel network via taps or any other sniffing tools. SNMP read-only access to Fibre Channel infrastructure is required for RISC Networks to collect information.

CISCO Discovery Services

RISC Networks utilizes Cisco Discovery Services (CDS) in order to obtain more specific information regarding Cisco infrastructure at a customer site. RISC Networks, Cisco and Cisco partners respect that customers are concerned about their privacy and network security and may be apprehensive about allowing an engineer to use a network assessment tool to discover data from their network and subsequently upload the data to Cisco using Cisco Discovery Service (CDS) for data analysis.

Cisco and RISC Networks have implemented several mechanisms to ensure customer data security. In addition, you will be required to accept an “Authorization to Proceed” (ATP) agreement before RISC Networks will upload data to Cisco CDS. An ATP helps ensure protection of customer data and specifically prohibits the dissemination of such data, providing assurance that neither Cisco nor RISC Networks will share or divulge customer data. Customers should be advised that data will be used only for the purpose of network analysis.
Show Commands used for Cisco Discovery Services:

- Show version
- Show inventory
- Show diag
- Show hardware
- Show module
- Show IDPROM all
- Show mls qos
- Show mls qos interface
- Show mls qos interface statistics
- Show policy-map interface
- Show running-config
- Show configuration

Once inventory data is collected by RISC Networks, if requested by the customer, it will be uploaded to Cisco Systems’ CDS application at the following URL: https://wsgx.cisco.com.

**Transferring the Data**

If utilizing CDS for analysis, customer network data is transferred from RISC Networks’ virtual assessment to Cisco using a secure HTTPS protocol to an internal Cisco CDS web service gateway where it is processed to provide detailed EoX, PSIRT, field notice and service coverage analysis.

Before transferring data to Cisco for analysis, passwords and security credentials are stripped from the data. To view a list of password scrubbing commands, please click here. SNMP data does not contain passwords or other sensitive configuration information. Instead of using IP addresses or host names to identify a device, a generic Device ID will be assigned. After processing, the analyzed data is transferred back to RISC Networks virtual assessment onsite at the customer using the same secure HTTPS protocols. It is then uploaded to the RISC Networks’ NAC as part of normal data upload procedures and used to generate the network analytics reports.

**Storing the Data**

The raw discovery data and analyzed XML report data are stored in a secure Cisco database behind Cisco’s firewall. The data is accessible only to CDS administrators for troubleshooting purposes. Other Cisco personnel may have limited access to high level transaction reporting that does not include customer inventory details.

All data is stored and eventually archived unless purging is specifically requested by the customer. The customer’s data is only accessible by Cisco or the partner who initiated the engagement.

Data for “Know the Network” (KTN), or service coverage reports, if requested, is also securely stored in Cisco databases behind the firewall. KTN reports are available only to the engineer who initiated the engagement and the Cisco service account team.
Purging Customer Data from Cisco Databases

The data obtained in the discovery process and uploaded to Cisco for processing can be deleted from Cisco’s database if requested by the Customer.

If service coverage reports were requested, the KTN data and reports need to be purged separately from the KTN portal (http://tools.cisco.com/ktn/). KTN data can be deleted from the report view.

Partner-Specific Security Issues – Discovery information will not be sold or distributed to anyone outside of Cisco, or used for direct marketing purposes.

Traffic Sim Instructions Setup

For instructions on Traffic Sim setup, see the following sections:

- Traffic Sim Setup Checklist
- RN50 Setup

Traffic Sim Setup Checklist

The following table is a checklist for Traffic Sim setup.

<table>
<thead>
<tr>
<th>Table 2-36 • Checklist for Traffic Sim Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Virtual RN150 Appliance</td>
</tr>
<tr>
<td>Required Ports between the RN50 and the RN150</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Required Ports between the RN50s</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Virtual RN50 Appliances (Requires at least 2)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Hypervisors</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Alternate and Additional Deployment Methods

1. **Initial Setup**
   
2. **Setting Up the Calls**
   
3. **Node Entitlement**
   
4. **Schedule the Simulation**
   
5. **Tips**

### RN50 Setup

To perform RN50 setup for Traffic Sim, perform the following tasks.

- **Initial Setup**

**Task** To perform RN50 setup for Traffic Sim:

1. Create the assessment on our portal. (RISC Networks portal)
2. Complete setup of the virtual RN150 and select ‘Start Assessment’.
3. Log on to https://cs-portal.riscnetworks.com
4. Select ‘TrafficSim’ in the ‘Collect Data’ dropdown menu
5. Download the virtual RN50 from our portal and unpack the zipped file to a folder
6. Deploy on a workstation or laptop with VMware Player (Free) or VMware Workstation
   
   **OR**

   7. Deploy to an ESX Server with VMware Vsphere Client or VMware Workstation
7. Power on / play the Virtual Machine
8. If you wish to continue with DHCP IP address, continue to step 6.
10. Select ‘Interfaces’
11. For setting static IP address, select static in dropdown box.
12. Enter IP information and select ‘Save’

### System Resources

- 2 Gigabytes of memory to allocate to the appliance
- 5 Gigabytes of Hard Drive Space

### Table 2-36 • Checklist for Traffic Sim Setup

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Resources</td>
<td>• 2 Gigabytes of memory to allocate to the appliance</td>
</tr>
<tr>
<td></td>
<td>• 5 Gigabytes of Hard Drive Space</td>
</tr>
</tbody>
</table>

*Note • To see what the codecs look like, see TrafficSim Codecs.*
13. Select ‘Dashboard’
14. Select ‘RN150’
15. Enter the IP address of the virtual RN150 appliance

**Setting Up the Calls**
To set up the calls, perform the following steps:

<table>
<thead>
<tr>
<th>Task</th>
<th>To set up the calls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log on to <a href="https://cs-portal.riscnetworks.com">https://cs-portal.riscnetworks.com</a> and find the tile for the assessment you wish to perform TrafficSim on</td>
</tr>
<tr>
<td>2.</td>
<td>Select “TrafficSim” at the bottom of the assessment</td>
</tr>
</tbody>
</table>

**Node Entitlement**
To set up node entitlement, perform the following steps:

<table>
<thead>
<tr>
<th>Task</th>
<th>To set up node entitlement:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select the virtual RN50 nodes to include in the call simulation. Nodes will automatically become enabled as they are added up to your entitlement.</td>
</tr>
<tr>
<td>2.</td>
<td>Purchase additional nodes if needed by selecting ‘Add Nodes’</td>
</tr>
</tbody>
</table>

**Schedule the Simulation**
To schedule the simulation, perform the following steps:

<table>
<thead>
<tr>
<th>Task</th>
<th>To schedule the simulation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select “Add New Operation”</td>
</tr>
<tr>
<td>2.</td>
<td>Select the desired time in UTC for the simulation. Current UTC time is displayed for convenience.</td>
</tr>
<tr>
<td>3.</td>
<td>Select “Get Available Devices for Selected Dates”</td>
</tr>
<tr>
<td>4.</td>
<td>Choose the Source and Destination nodes (simulations are run bidirectional)</td>
</tr>
<tr>
<td>5.</td>
<td>Select the “Codec” and “QoS Value”</td>
</tr>
<tr>
<td>6.</td>
<td>Select the “Get Capacity of Selected Devices”</td>
</tr>
<tr>
<td>7.</td>
<td>Select the number of calls and the duration</td>
</tr>
<tr>
<td>8.</td>
<td>Enter a description for the call simulation. This will allow for easy identification of the operation in the final report.</td>
</tr>
<tr>
<td>9.</td>
<td>(Optional) Select the “Advanced Config” to manually set the thresholds and control the auto pause feature. (Default settings will cause Auto-pause feature to pause the simulation if it exceeds 10% packet loss)</td>
</tr>
<tr>
<td>10.</td>
<td>Select “Create Operation” to begin the simulation.</td>
</tr>
</tbody>
</table>
After the call simulation has been created, the assessment will initiate very lightweight test calls between the virtual RN50s to verify communication between the involved devices. Notifications will be sent updating the user on the status of the test including what, if any, required ports were closed, and whether or not DSCP values were maintained.

**Tips**

Note the following tips regarding Traffic Sim:

- TrafficSim operations run on 5 minute intervals for the set duration (30 or 60 seconds.)
- The RN150 appliance is not eligible as a simulation node. All simulations are run bidirectionally between the RN50 appliances. (you will need to deploy an RN50 to each site you wish to simulate to and from.
- TrafficSim simulations run bidirectional. If you set up a call from site A to site B, you will NOT need to set up a 2nd operation from site B back to site A.
- We recommend running simulations 24 – 48 hours. This will provide greater visibility into Jitter, Loss, and Delay at times of the day.
- The Auto-pause feature will pause the simulation if 10% packet loss is exceeded. This value can be manually adjusted in the Advanced Config section.
- It is recommended to place the RN50 on the correct VLAN for Voice, Video, or Data. This will allow you to verify QoS in the environment.
- The RN50 does NOT need internet access to our NOC servers as the RN150 does.
- The RN50s and the RN150 do NOT need to be in scope (included in the subnet ranges at time of setup)

**TrafficSim Codecs**

This section describes the following TrafficSim Codecs:

- G.729.2
- G.711.2
- 720
- 1080
- RTAudioNarrow
- RTAudioWide
- RTAudioNarrowFEC
- RTAudioWideFEC
- RTAudioWideFEC
G.729.2

An audio data compression algorithm for voice that compresses digital voice in packets of 10 milliseconds duration. It is a Low Bit Rate Codec at approximately 26 Kbps.

Table 2-37 • G.729.2 Codecs

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Captured</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>Between First and Last Packet</td>
<td>59.975 sec</td>
<td></td>
</tr>
<tr>
<td>Avg. Packets/sec</td>
<td>50.021</td>
<td></td>
</tr>
<tr>
<td>Avg. Packet Size</td>
<td>74.000 bytes</td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>222000</td>
<td></td>
</tr>
<tr>
<td>Avg. Bytes/sec</td>
<td>3701.520</td>
<td></td>
</tr>
<tr>
<td>Avg. MBit/sec</td>
<td>0.030</td>
<td></td>
</tr>
</tbody>
</table>

Download

Click here to Download a PCAP.

This file contains one direction of a 60-second G.729.2 call.
**G.711.2**

G.711ulaw, also known as Pulse Code Modulation, is a narrowband audio codec mostly used in Voice over Internet Protocol, that provides toll-quality audio at 80 kbit/s.

**Table 2-38 • G.711.2 Codecs**

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Captured</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>Between First and Last Packet</td>
<td>59.975 sec</td>
<td></td>
</tr>
<tr>
<td>Avg. Packets/sec</td>
<td>50.021</td>
<td></td>
</tr>
<tr>
<td>Avg. Packet Size</td>
<td>214.000 bytes</td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>642000</td>
<td></td>
</tr>
<tr>
<td>Avg. Bytes/sec</td>
<td>10704.427</td>
<td></td>
</tr>
<tr>
<td>Avg. MBit/sec</td>
<td>0.086</td>
<td></td>
</tr>
</tbody>
</table>

**Download**

Click here to Download a PCAP.

This file contains one direction of a 60-second G.711.2 call.

**720**

This is a 720 resolution video call.

**Table 2-39 • 720 Codecs**

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Captured</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>12631</td>
<td></td>
</tr>
<tr>
<td>Between First and Last Packet</td>
<td>59.987 sec</td>
<td></td>
</tr>
<tr>
<td>Avg. Packets/sec</td>
<td>210.562</td>
<td></td>
</tr>
<tr>
<td>Avg. Packet Size</td>
<td>1141.248 bytes</td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>14415107</td>
<td></td>
</tr>
<tr>
<td>Avg. Bytes/sec</td>
<td>240303.504</td>
<td></td>
</tr>
<tr>
<td>Avg. MBit/sec</td>
<td>1.922</td>
<td></td>
</tr>
</tbody>
</table>
Download

Click here to Download a PCAP.

This file contains one direction of a 60-second 720 call.

1080

This file contains a 1080 resolution video call.

Table 2-40 • 1080 Codecs

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Traffic Captured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packets 48362</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between First and Last Packet 59.994 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packets/sec 806.110</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packet Size 783.867 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bytes 37909389</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Bytes/sec 631883.085</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. MBit/sec 5.055</td>
</tr>
</tbody>
</table>
**RTAudioNarrow**

This file contains one direction 60 second RTAudioNarrow call.

### Table 2-41 • RTAudioNarrow Codecs

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Traffic Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packets 3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between First and Last Packet 59.977 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packets/sec 50.019</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packet Size 113.0 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bytes 339000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Bytes/sec 5652.197</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. MBit/sec 0.045</td>
</tr>
</tbody>
</table>

**Download**

Click here to [Download a PCAP](#).

This file contains one direction of a 60-second RTAudioNarrow call.

**RTAudioWide**

This file contains one direction 60 second RTAudioWide call.

### Table 2-42 • RTAudioWide Codecs

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Traffic Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packets 3000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Between First and Last Packet 59.977 sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packets/sec 5.019</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Packet Size 156,000 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bytes 468000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. Bytes/sec 7802.983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg. MBit/sec 0.062</td>
</tr>
</tbody>
</table>
Download

Click here to Download a PCAP.

This file contains one direction of a 60-second RTAudioWide call.

**RTAudioNarrowFEC**

This file contains one direction 60 second RTAudioNarrowFEC Call

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Traffic Capture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 2-43 • RTAudioNarrowFEC Codecs**

<table>
<thead>
<tr>
<th>Summary</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>3000</td>
</tr>
<tr>
<td>Between First and Last Packet</td>
<td>59.977 sec</td>
</tr>
<tr>
<td>Avg. Packets/sec</td>
<td>50.019</td>
</tr>
<tr>
<td>Avg. Packet Size</td>
<td>143.0 bytes</td>
</tr>
<tr>
<td>Bytes</td>
<td>429000</td>
</tr>
<tr>
<td>Avg. Bytes/sec</td>
<td>7152.781</td>
</tr>
<tr>
<td>Avg. MBit/sec</td>
<td>0.057</td>
</tr>
</tbody>
</table>

Download

Click here to Download a PCAP.

This file contains one direction of a 60-second RTAudioNarrowFEC call.
RTAudioWideFEC

This file contains one direction 60 second RTAudioWideFEC Call

Table 2-44 • RTAudioWideFEC Codecs

<table>
<thead>
<tr>
<th>Bits</th>
<th>Packets</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>Capture</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>Between First and Last Packet</td>
<td>59.977 sec</td>
<td></td>
</tr>
<tr>
<td>Avg. Packets/sec</td>
<td>50.019</td>
<td></td>
</tr>
<tr>
<td>Avg. Packet Size</td>
<td>229.000 bytes</td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>687000</td>
<td></td>
</tr>
<tr>
<td>Avg. Bytes/sec</td>
<td>11454.463</td>
<td></td>
</tr>
<tr>
<td>Avg. MBit/sec</td>
<td>0.092</td>
<td></td>
</tr>
</tbody>
</table>

Download

Click here to Download a PCAP.

This file contains one direction of a 60-second RTAudioWideFEC call.

Appliance Certificate Management

Note • The Certificate Management feature is currently only available for the FlexDeploy Appliance.

Note • This document refers to SSL (Secure Sockets Layer) as well as TLS (Transport Layer Security) generically as SSL. All appliance services using HTTPS will use TLS 1.2.

The Certificate Management feature allows users to supply a custom SSL certificate and private key for installation into a RISC Networks Appliance. By default, appliances use a self-signed SSL certificate and key pair that is generated during the bootstrap procedure. While this ensures that communication with the appliance via a web browser is encrypted, providing security and integrity of the transmitted data, it does not provide confirmation of identity between the client and the appliance, and results in a security warning when connecting. With Certificate Management, a certificate trusted either by the global PKI infrastructure or by internal Certificate Authorities, can be installed on the appliance. This provides confirmation of identity and removes the security warning.

- Using the Feature
- Certificate Format
Important • RISC Networks does not guarantee the function of users' PKI related to the installation of a custom certificate. In particular, any issues related to the trust of an installed custom certificate are the responsibility of the user to resolve.

Using the Feature

To access the Credential Management feature, browse to the FlexDeploy appliance’s configuration application, log in, and access the Interfaces page. The Certificate Management button can be found below the network interface configuration section. Next to the button will be a tag describing whether the default certificate (the self-signed automatically generated certificate), or a user supplied custom certificate is currently installed. Select the Certificate Management button.

Once viewing the Certificate Management page, detailed information about the currently installed certificate can be accessed using the View Certificate button. This will provide details such as the identity of the issuing certificate and the identity of the server certificate.

To install a custom certificate and key, populate the form fields in the Install a Custom Certificate section and select Verify And Apply. On the dialog, first select Verify. This will check the provided Server Name, Certificate Chain, and Server Key data to ensure that the configuration is correct. If the configuration does not pass the verification process, an error will be shown and the certificate and key will not be installed. If the configuration passes the verification process, selecting the Apply button will install the certificate and key on the system, and restart system services to begin using the new configuration.

If you would like to remove a custom certificate that has been installed, the Roll Back To Default button can be selected. This will remove the custom certificate and key from the appliance, install the default certificate and key, and restart the system services to use the default configuration. Once Roll Back To Default is selected, you will be asked to confirm that you would like to proceed with the operation. Once completed, in order to return to a custom certificate it will need to be re-entered and installed.

Figure 2-5: Certificate Management
Certificate Format

The certificate and private keys provided for the Certificate Management feature have several requirements. Before installing a certificate and key, a verification process is run to confirm that these requirements are met.

- Certificates and private keys must be encoded in the PEM format
- Certificates and private keys must be compatible with OpenSSL and the Apache Web Server
- The certificate and key must match each other
- The Common Name of the certificate must match the Server Name provided in the configuration
- The certificate must be a valid chain, containing the server certificate as well as any required signing certificates
- The certificate chain must be ordered in terms of the trust chain from leaf to root, or server certificate to the root certificate

First, certificates and keys must be provided in the text-based PEM encoding. This format uses the Base64 text encoding to represent the certificate or key data, and contains header and footer lines describing the type of data it contains. The header and footer lines should be included in the certificate and key data when entering them into the Certificate Management feature.

The RISC Networks Appliances use the Apache Web Server and the OpenSSL cryptographic framework to provide HTTPS services. Certificates and keys provided for the feature must be compatible with this software stack. For more advanced compatibility concerns, please consult the upstream documentation for these projects. Links are available at the bottom of this page.

The server certificate contains a "subject" line describing the identity of the server, including a Common Name (CN) that identifies its name. When accessing the web application, the name used to contact the server must match the Common Name of the certificate it presents. Otherwise, an warning is issued by the browser. The Server Name field defined in a custom certificate installation must match the Common Name of the server certificate, which should also match the DNS name used to initiate a connection to the appliance. If the Server Name field does not match the Common Name of the certificate, the verification process will produce an error and the installation will not proceed.

The Certificate Management feature does not accept the certificate trust chain as a separate file. The Certificate Chain provided when installing a custom certificate must contain all certificates participating in the trust chain. Typically, this constitutes the server certificate, one or more intermediate signing certificates, and a root Certificate Authority certificate. If your PKI infrastructure currently has the CA bundle separate from the server certificate, they can be concatenated together into a single file. The order of certificates in the chain must be ordered from leaf to root, meaning the server certificate is the first entry in the file, followed by any intermediate signing certificates, and finally the root certificate. If the chain is not ordered in this way, the verification process will fail, typically due to the Server Name not matching the Common Name of the certificate, and installation will not proceed.
Examples

The following shows a valid certificate chain, including a server certificate, an intermediate signing certificate, and a root certificate, and the corresponding private key:

Example Certificate Chain

Example Private Key

External Links

For more information on appliance certificate management, see the following:

- OpenSSL
- Apache Web Server SSL/TLS Encryption

Appliance NTP Support

Note • NTP support is only present on the latest RN150 images named like RISC_Networks_RN150_YYYY-MM-DD.zip. These have been available for download since 2020-09-01.

To learn about Foundation and Cloudscape Appliance NTP support, see the following sections:

- Overview of Appliance NTP Support
- Configuring NTP on the Virtual Appliance
- NTP Configuration Values

Overview of Appliance NTP Support

The RISC Networks Virtual Appliances require the time and date to be accurate in order to correctly display collection scan times in the platform, for HTTPS to work properly, and for appliance software updates to be validated.

The NTP (Network Time Protocol) client is enabled by default on the RN150 appliance. There are two NTP servers hosted in the RISC Networks SaaS environment reachable via ntp.riscnetworks.com. Accordingly, outbound internet connectivity to ntp.riscnetworks.com (3.231.5.12 and 18.204.38.15) on UDP port 123 should be allowed in order for the RN150 to synchronize time.

In some circumstances, for example when all internet-bound traffic must be routed through a proxy, it may not be possible to enable the aforementioned outbound connectivity. There are two other options in this case.

The first is that the hostname/IP of the NTP server can be changed by visiting the Interfaces section of the RN150 configuration interface. If an intranet NTP server exists, it is recommended to configure the RN150 to use that.
Otherwise, NTP can be disabled completely in which case the RN150 will obtain its time from the VMware hypervisor that it is running in. It is important then that the hypervisor itself keeps accurate time. See VMware’s documentation on the subject for details on how to configure the hypervisor to synchronize time via NTP or manually.

## Configuring NTP on the Virtual Appliance

To configure NTP on the virtual appliance, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To configure NTP on the virtual appliance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Interfaces section of the RN150 configuration interface.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the Configure NTP button.</td>
</tr>
<tr>
<td>3.</td>
<td>Make any desired changes, and click Submit.</td>
</tr>
</tbody>
</table>

### Disabling the NTP Client

To disable the NTP client, and instead use hypervisor time, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To disable the NTP client:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Interfaces section of the RN150 configuration interface.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the Configure NTP button.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>

### Resetting to Default NTP Settings

To reset the NTP settings to defaults, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To reset to default NTP settings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Open the Interfaces section of the RN150 configuration interface.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the Configure NTP button.</td>
</tr>
<tr>
<td>3.</td>
<td>Click Defaults and then click Submit.</td>
</tr>
</tbody>
</table>
NTP Configuration Values

The NTP configuration dialog contains the following fields:

Table 2-45 • NTP Configuration Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Address</td>
<td>The hostname or IP address of the NTP server/pool.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>One of <strong>Server</strong> or <strong>Pool</strong>.</td>
</tr>
<tr>
<td>- Server should be selected when the specified hostname resolves to only a single IP address, or an IP address is used.</td>
<td></td>
</tr>
<tr>
<td>- Pool should be selected when the hostname resolves to more than one IP address. For example, ntp.riscnetworks.com is a pool. A commonly used public pool is pool.ntp.org (<a href="https://www.ntppool.org">https://www.ntppool.org</a>).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>This will display one of several statuses depending on the state of the appliance NTP client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- <strong>Enabled (Healthy)</strong> will show when the appliance is successfully syncing to an NTP server or pool.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Enabled (Not yet synchronized)</strong> will show when NTP is enabled, but the appliance has not yet synchronized its time. It can occur for one of a few reasons:</td>
<td></td>
</tr>
<tr>
<td>- This may show for some time after a new configuration is applied or the appliance is rebooted.</td>
<td></td>
</tr>
<tr>
<td>- This may show if the specified NTP server/pool is not reachable due to a firewall or other connectivity issue.</td>
<td></td>
</tr>
<tr>
<td>- This may show if there is connectivity to the specified server/pool, but the local client is rejecting the provided time due to instability or inconsistency.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Disabled (ESXi Host timesync in use)</strong> will show if NTP is disabled.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Enabled (Error: unable to communicate with daemon)</strong> will show in the unlikely case that the local NTP client is not running or reachable. Reapplying the settings (via Submit) may fix this, but if not, it is recommended to reach out to support.</td>
<td></td>
</tr>
<tr>
<td>- <strong>Enabled (Error: status check failed)</strong> will show in the unlikely case that an unknown error has occurred when attempting to query the status of the NTP client. It is recommended to reach out to support if this occurs.</td>
<td></td>
</tr>
</tbody>
</table>

| Appliance Time | This shows the current time from the appliance’s perspective. The displayed time will refresh approximately every 5 seconds. |
This section explains how to deploy the virtual appliance, perform complete discovery with proper troubleshooting, and proceed to the performance collection phase successfully.

- **Predeployment Checklist**
- **Quick Start Guide**
- **Discovery: How To**
- **Discovery Troubleshooting**

## Predeployment Checklist

The following checklist covers everything you should review and prepare for prior to beginning a RISC Networks engagement.

**Table 3-1 • Predeployment Checklist**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Ready (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the Operations and Security information found at the following links:</td>
<td>Yes</td>
</tr>
<tr>
<td>• Architecture, Data Handling, and Security</td>
<td></td>
</tr>
<tr>
<td>• What We Collect</td>
<td></td>
</tr>
<tr>
<td>• How We Collect</td>
<td></td>
</tr>
<tr>
<td>Review the Deployment Requirements for information on resource, network, and credential requirements of the virtual appliance:</td>
<td>Yes</td>
</tr>
<tr>
<td>• Deployment Requirements</td>
<td></td>
</tr>
<tr>
<td>VMware platform with the necessary resources available for RN150 deployment (ESXi, VMware Workstation, VM Player).</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Quick Start Guide

New to RISC Networks? Use this guide to get started with the Foundation and CloudScape platform.

Getting started with the Foundation and CloudScape platform is quick and easy. The setup process generally takes between 5 minutes to an hour, depending on the number of credentials you have for your environment.

- **Prerequisites**
- **Create an Assessment**
- **Deploy the RN150**
- **Log In to the RN150**
- **Enter Your Assessment Key**
- **Enter Subnet Information**
• Enter SNMP Information
• Enter Windows Credentials
• Enter VMWare Credentials
• Enter SSH Credentials
• Additional Credentials
• Additional Features
• Complete Bootstrap and Start Scan
• Review Assets and Request Rescan
• License Devices for Data Collection
• Next Steps

Prerequisites

Review/complete the [Predeployment Checklist](#).

In addition to our quick start guide below, we offer professional services. For more information on professional services please contact info@riscnetworks.com.

⚠️ Important • All RISC Networks engagements require a subscription and licenses. If you do not have a subscription, contact [Account Management](#). If you have a subscription and need to purchase node licenses, please contact your account manager or contact [help@riscnetworks.com](mailto:help@riscnetworks.com).

Create an Assessment

The first step to using the Foundation and CloudScape platform is to create an assessment. Follow the instructions below to get started.

### Task

<table>
<thead>
<tr>
<th>To create an assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to the RISC Networks Portal.</td>
</tr>
<tr>
<td>2. Log in, or register if you don’t already have an account.</td>
</tr>
<tr>
<td>3. Click the <strong>Add an Assessment</strong> button in the assessment list window.</td>
</tr>
<tr>
<td>4. Enter your subscription code in the field. If you do not have a subscription code, please reach out to your account manager or to <a href="mailto:info@riscnetworks.com">info@riscnetworks.com</a>.</td>
</tr>
<tr>
<td>5. Fill in the company information fields in the <strong>Add an Assessment</strong> window, company name will be the name of the assessment.</td>
</tr>
</tbody>
</table>
6. To invite other users, click the **Invite** button. You will be taken to the **User Access** screen, where invitations can be sent via email. Users can also be invited later on. Click **Dashboard** to return to the main screen.

7. Upon completion, you should see a pane with your new assessment.

## Deploy the RN150

In order to start discovery we need to download and deploy the RISC Networks RN150 virtual appliance.

### Task

**To deploy the RN150 virtual appliance:**

1. Click your assessment to open the **Appliance Status** page.
2. Click the **Download RN150** button in the section titled: **Step 1 - Download Virtual Appliance**.
3. While waiting on your download to complete, copy the code provided in the section **Step 2 - Bootstrap Virtual Appliance with the Code** in the Appliance Status page, and save it where you can retrieve it at a later time.
4. When your download completes, extract the files to a safe place.
5. Follow VMware documented procedures for Deploying OVF Templates in your specific version of VMware.
   - **Deploy OVF Template Using VI Client in vSphere 5.1**
   - **Deploy OVF Template Using Web Client in vSphere 5.5**
   - **Deploy OVF Template Using VMware Player**
6. Once the machine is deployed and powered on, you should see the RISC Networks Logo and briefly see a white screen before being redirected to a log in screen.

**Note** • For more information, see **Deployment Requirements**.

## Log In to the RN150

After powering on the RN150, you can log in and accept the RISC Networks End User License Agreement. In the top right corner of the page is the IP address of the appliance which can then be navigated to via a web browser. We recommend accessing the RN150 through your web browser as copy/paste may not be available through the hypervisor console. Open your browser of choice and navigate to the IP address. Once the site has loaded, you can close the hypervisor console. Follow the instructions below to log in.

### Task

**To login to the RN150:**

1. Enter your username (Email address).
2. Enter your password.
3. Go to the box on the right to read the eula. Scroll to the bottom.
4. Elect whether or not use professional services.
5. Accept the End User License Agreement.
6. Click Login.

Enter Your Assessment Key

Now it is time to enter the assessment key we copied in Deploy the RN150 above. Again, we recommend using the RN150 in a browser window because copy/paste may not be available in a hypervisor console.

Task | To enter your assessment key:
--- | ---
1. Enter your assessment key.
2. You will be prompted to choose whether or not you are using FlexDeploy. If you are unsure, click No.
3. If you are using FlexDeploy, enter the network address of the FlexDeploy appliance you have previously set up.

Enter Subnet Information

Now it is time to enter Subnet information. We can’t go any further without entering at least one subnet. There are three options for entering subnet information. You can enter a subnet individually, populate from a routing table, or populate from a .csv file.

Task | To enter subnet information:
--- | ---
1. Click the Subnets link on the Dashboard page.
2. To enter subnets individually, enter a network address >> select Subnet Mask from the dropdown >> Click Add.
3. To populate from a routing table, click Populate from routing table >> at the prompt, select the version of SNMP you are using >> enter your credentials.
4. To enter subnets using a .csv file, click Populate from CSV >> click Choose File and browse to your subnets.csv file >> select the file and click Open, and click Upload.

Note • The file must be under 1MB and formatted as either network address/CIDR prefix, or network address/CIDR prefix new line. (ex. 63.146.167.192/26,65.125.73.180/30)
5. In the table below, make sure to select all of the subnets you wish to scan.
6. After you have confirmed that you have selected all subnets for which you want information, click the Dashboard button.
Enter SNMP Information

To enter SNMP information, perform the following steps.

Task  To enter SNMP information:

1. Click the SNMP link on the dashboard page.
2. Enter an SNMP string in the input box, or click the Add SNMP Version 3 button if you are using SNMP version 3 >> click Add
3. Enter the IP address. and click Test
4. After testing successfully, click OK and return to the dashboard

Enter Windows Credentials

Important • Be sure to enable netstat application socket collection in order to collect and view workload dependencies. Refer to Windows Collection Module for more information.

To enter Windows credentials, perform the following steps.

Task  To enter Windows credentials:

1. Click the Windows link on the Dashboard page.
2. Enter the domain for your credential, optional.
3. Enter your user name and password.
4. Select an option for application socket collection.
5. We recommend you select Enable >> confirm your choice >> click Next >> Select whether you want to enable this feature on workstations.
6. Click Add
7. Click Test to verify your credential. We recommend testing all credentials. This helps ensure we collect information on all relevant devices and prevents problems later on.
8. After receiving confirmation that your credential is correct, click OK and either add more credentials, or click the Dashboard button to go back to the main page.

Note • We recommend testing all credentials prior to starting a scan. This ensures information is collected on all relevant devices the first time, and that the complete set of analytics is available.
Enter VMWare Credentials

It is time to enter your VMWare credentials

**Task**

**To enter VMware credentials:**

1. Click the VMWare link on the Dashboard page.
2. Enter a network address.
3. Confirm you are hitting the right port. The default is port 443.
4. Enter a username and password
5. Click Add.
6. Click Test to verify your credential.
7. After receiving confirmation that your credential is correct, click OK and either add more credentials, or click the Dashboard button.

Enter SSH Credentials

It is time to enter your SSH credentials

**Task**

**To enter SSH credentials:**

1. Click the SSH link on the Dashboard page.
2. Enter the username for the credential in the Username field.
3. From the drop-down list entitled Credential Type, select the type of authentication desired.
   - If Password is selected, an additional entry field will be presented, in which the password should be entered.
   - If Public Key is selected, a text input field will be presented. The full text contents of the private key associated with the credential should be pasted here.
4. Click Add.
5. Click Test to verify your credential
6. After receiving confirmation that your credential is correct, click OK and either add more credentials, or click the Dashboard button.
Additional Credentials

The RN150 supports additional credentials under the sections Cisco CallManager, Cisco Discovery Services, and Additional Credentials.

The Additional Credentials sections can contain Database Credentials (as described in Database Module) if that is enabled, and CLI for Cisco Devices. If you have these credential types or if they are relevant to your desired analysis then please enter them, otherwise proceed to the next section.

Additional Features

There are additional RN150 features available to you on the Global Settings dialog box, which is accessed from the Assessment section of the RN150 Dashboard.

Task  
To set additional features on the Global Settings dialog box:

1. Open the RN150 Dashboard.
2. Click Assessment.

On the Global Settings dialog box, you can enable or disable the following features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrub Process Arguments</td>
<td>Enabling this option will remove or otherwise not collect the argument list for running processes for all devices. This can be used when process arguments may contain sensitive data.</td>
</tr>
</tbody>
</table>

Note: This will reduce the data available in the platform, and may impact application analysis.
Complete Bootstrap and Start Scan

After entering or opting out of all credential categories, You have the option to start the assessment.

Task

To complete bootstrap and start scan:

1. Click the Start Assessment button.
2. You will be prompted to confirm your settings. Confirm that all of the credentials you entered are accounted for in this pop up.
3. Click Start.

You have now completed the RN150 setup. You will receive an email when the discovery process is complete.

Review Assets and Request Rescan

You will receive an email notifying you that the scan is complete. Once you receive this email, you should review your assets to verify that all devices that are in-scope for the assessment are accessible.

Note • We have more detailed documentation on the discovery troubleshooting and the process in general in Discovery: How To. We recommend reviewing this page before proceeding so you understand the resources available.
Task: To review assets and request rescan:

2. Click the **Consume Intelligence** dropdown >> click **Assets**.
3. Verify all devices and subnets are in scope and in scope devices are accessible (i.e. Make sure Windows Servers are in the “Windows Devices” section and not under “Inaccessible Devices”).
4. If needed, go back to the RISC Networks RN150 appliance and add missing credentials and click the Request Rescan button as needed.

License Devices for Data Collection

Now it is time to license devices in your network to start data collection. You may or may not want to license everything. For instance, you may want to license **Windows Servers** only or, devices in a certain ip range. You can do this by filtering the list of devices in the licensing page. Generally, it is recommended that all devices whose device type contains "server" should be licensed. These are devices that we are collecting both performance and dependency data on as we have OS level access.

Task: To license devices for data collection:

2. Click the **Collect Data** dropdown >> click **Licensing**.
3. On the **Core Licensing** tab, filter to the devices you would like to license (you can apply filters by clicking the down arrow in a column header and enter a filter value).
4. Depending on your subscription you may need to select the Start 30 Day Burst button to make your licensing available (this activates a clock which makes the burst licensing available for 30 days)
5. To license check the **License** box.
6. Devices will start collecting as soon as they are checked. Uncheck the device to remove it from collecting.

Next Steps

You have completed the quick start. After you have collected a sufficient amount of performance and dependency data it will be time to proceed to the Application Review Process.

For more information, see Building Application Stacks.
Discovery: How To

Information about discovery is described in the following sections:

- Understanding the Asset Report
- Discovery Troubleshooting
- Discovery Scheduling

Understanding the Asset Report

The Assets page (located underneath Consume Intelligence > Assets) of the platform is meant to be your working page for reviewing the discovery results and taking further action. The Assets page is meant to be a listing of devices discovered within the customer environment. It should be used in an iterative process for scope setting/discovery of the customer’s environment (i.e. it is used as a working document throughout multiple scans to troubleshoot and discover further areas of a customer’s environment until the target scope is achieved).

**Important** • Review How We Collect to gain a more in-depth understanding of the discovery process/what the appliance is doing.

The Asset Report is generated after the RN150 has completed the inventory phase. The appliance/assessment always works in this manner:

The Asset Report lists all devices that responded to an ICMP ping. Additionally, if we were able to connect to them using the provided credentials and categorize them they are further classified into devices types (as described in Device Type Definitions), such as Windows Server, Windows Workstation, etc). Each category in the Asset Report aligns to a specific credential input into the appliance. (i.e. Devices under the Windows Server link indicate we have WMI access to that box, the Linux/Unix link shows SNMP or SSH accessible devices, if it is in the Virtual Machine link we have vCenter access, etc.). Clicking each link will filter the table below to show just those devices.

**Key Takeaways**

- **The report is additive.** With each successive rescans of the environment the newly discovered data will be added to that of the previous scan. Data is never removed, even in the event that credentials or subnets are removed or deselected for scanning in the appliance.

- **There is often overlap between the links.** Since they correspond to a credential we could have a Windows VM that is in both the Windows link and the VM link as it responded to both sets of credentials (Windows Admin and vCenter). Additionally, it can be in the inaccessible devices link if one credential worked, but not another (e.g. vCenter passed, but Windows failed). Please note that the Foundation and CloudScape platform will resolve the duplicate devices when doing subsequent reporting (you will only see one device for the VM and Windows Server), but the asset report is purposefully left as-is so that virtual teams and windows teams can both confirm the expected asset list.
Discovery Troubleshooting

As you work with the customer on scope setting you will undoubtedly spend time reviewing inaccessible devices. Devices end up in this category because at least one set of applicable credentials were attempted and were unable to gain access to the device(s). During the inventory phase we look to see what ports are open on a specific host. If we see ports for WMI or SNMP open then we will attempt to use the corresponding credential.

Generally, it is best to focus on those devices that are identified in the MAC manufacturer as common server or VM manufacturers (VM Ware, HP, Dell, etc.). We will uncover any device in the environment that responds to ICMP ping, so there can be many devices in this tab that are not in scope or useful to your objective.

Lastly, in many cases customers may not be sure the scope is correct. That’s okay, this is an iterative process and is designed such that we can always come back and rescan. You may find, once you have collected performance data on the scope and started working on grouping applications, traffic going to IPs that are out of scope. This is covered in our Application Grouping Workflow document, but know that discovery can be an iterative process. You will get further data to help you disposition the environment as you continue in the assessment process. Think of it as you are illuminating a dark room; it is not possible to fully light the room without understanding how big it is. Start with what you have so you can use it to illuminate other dark corners of a customer’s environment.

For detailed troubleshooting instructions and error messages please refer to the Troubleshooting subsections of the following collection modules:

- Windows Collection Module
- SSH Collection Module

Discovery Scheduling

Note • All times used in the Discovery Scheduling feature use the UTC time zone, including the calendar views and the time of day for scheduled scans.

Note • Discovery Scheduling feature is not available for legacy IT HealthCheck subscriptions.

Regularly doing a discovery on an environment captures any changes (new servers or VMs stood up or spun down).

- Scheduling a Discovery Scan
- Scanning Behavior

Scheduling a Discovery Scan

The Discovery Scheduling feature becomes available after the initial scan of the environment has been requested. Following the initial scan, the Schedule Rescans button will appear next to the Request Rescan button on the RN150 Dashboard page.
Figure 3-1: Schedule Rescans Button

Selecting the Schedule Rescans button will open the Discovery Scheduler page. This page provides a calendar view of the current month showing the currently scheduled Discoveries. You can navigate forwards and backwards through months of the year using the < and > buttons on the top right of the calendar view. The Today button will navigate back to the current month with the current day highlighted.

Selecting the + Add button will open a dialog for scheduling a new Discovery scan. You can modify any existing scheduled Discovery scan by clicking on an entry shown in the calendar.

Scanning Behavior

**Note** • When the appliance is in discovery mode it IS NOT collecting performance data. To maintain appropriate balance between performance collection and discovery we recommend scheduling discoveries no more frequent than once every couple of days. Often a weekly schedule may be optimal.

A scheduled scan acts exactly the same as if the Request Rescan button had been selected from the RN150 Appliance Dashboard. The scan is requested at the time it was scheduled, and will begin running up to several minutes later. An email notification will be sent when the scan starts, and when the scan has completed and updated Assets information is available in the Portal or FlexDeploy Appliance. Scheduled scans always use the behavior as if the View Inventory Changes feature had been selected, which will refresh the data for Assets that have previously been inventoried as well as discovering any new devices. Note that the subnet scope used during a scheduled scan reflects the currently selected subnet entries in the RN150 Subnets page at the the scan is initiated.
If the RN150 Appliance does not have connectivity with the RISC Networks NOC (referred to as being “offline”) at the time the scan is scheduled, the scan will not be initiated and the RN150 Appliance will not attempt to run any scheduled scans that were missed when connectivity is resumed.

- **Adding A New Scheduled Discovery Scan**
- **Updating An Existing Scheduled Discovery Scan**

**Adding A New Scheduled Discovery Scan**

Select the + Add button at the top right of the calendar to open the Schedule A Discovery dialog for adding a new Discovery scan to the schedule.

Selecting the Run Date input field will open a calendar where the day can be selected. A Discovery cannot be scheduled in the past, so days prior to the current day, and months prior to the current month, cannot be selected. Click on the desired day to request the scan.

Next, select the time of day to request the scan, in the UTC time zone. The minutes field shows a range of times in 15 minute increments. A range is shown to indicate the asynchronous nature of scan requests. The scan will be requested at the beginning of the time range (for instance, if the 30-45 minute range is selected, the scan will be requested at the 30th minute of the hour, but the scan will actually begin running up to several minutes later.

To schedule a single Discovery scan, leave the Repeat Every field at the default value of 0. If you would like to schedule a routine, recurring scan, the Repeat Every value should be set to the number of days between requests. For instance, to request a weekly rescan on the same day of the week, set the Repeat Every value to 7. The selected hour and minute of the day will be used for each scan request initiated in the series.

Select Add to complete the configuration and add the new scan(s) to the schedule. The new scans will now appear in the calendar view on the page. The Cancel button can be selected at any time before selecting Add to quit configuration, which will not add the scan(s) to the schedule.

**Updating An Existing Scheduled Discovery Scan**

From the main calendar view, click on the calendar entry that you would like to change. This will open the Edit A Scheduled Discovery dialog. From this dialog, any parameter of the scheduled scan can be manipulated, including the day, time of day, and recurrence. To finalize any changes, select Update. If you would like to permanently remove the scan from the schedule, select Delete. Selecting Cancel will close the dialog without making any changes to the schedule.

When editing a scheduled scan that is part of a recurring series (the Repeat Every value is greater than zero), note that any changes made to a scheduled scan in the series operates on the series as a whole. This means that changing the time of day on any element of the series will change the time of day for all subsequent scans, changing the Repeat Every recurrence value will change the interval between all scans in the series (beginning from the original scan in the series), and selecting Delete will remove all entries part of that series.

Note that scheduled scans that have already occurred cannot be modified.
Discovery Troubleshooting

Information about discovery troubleshooting is described in the following sections:

- Collection Validation
- Protocol Specific Troubleshooting
- Discovery Help

Collection Validation

The Collection Validation feature is the primary troubleshooting tool for issues relating to data collection for Discovery or Performance collection.

The Collection Validation feature is available on the RN150 Virtual Appliance. It allows the user an in-depth review of what data collection activities are performed against a device, and details about any operations that are not successful. The Collection Validation feature is a compliment to the existing Credential Test feature on the RN150, and a crucial part of troubleshooting during the Discovery stage of an engagement.

Currently, the Collection Validation feature is only available for the SSH Collection Module, for Linux/UNIX devices using SSH, and for the Windows Collection module, using the WMI and SMB protocols for collection from Windows servers and workstations.

- Credential Test
- Collection Validation
- Overall Status
- Result Codes
- Failure Details
- Common Issues Resulting In A PARTIAL Status
- Common Issues Resulting In An ERROR Status

Credential Test

For each credential type, the Test button is available when entering a new credential or editing an existing credential. The Credential Test feature accepts the IP address of a device, and runs a simple connection and authentication test against that device using the credential entry being operated on. The Credential Test does not test whether the device will respond to ICMP, and only runs the minimum operations required to confirm whether the credential can be used to communicate with the device. The Collection Validation feature has been introduced to go beyond this simple test and to provide extensive detailed feedback, although the Credential Test feature remains a valuable tool in many conditions. The Credential Test feature will, upon a successful test, automatically add the new credential entry or apply a modification to the existing credential entry.
Collection Validation

The Collection Validation feature, like the Credential Test, can be used when entering a new credential entry or editing an existing credential entry. Selecting the Validate button will open a dialog where the IP address of a device you would like to test against is entered. Once the validation process is complete, a report will be displayed on the screen detailing each operation that was performed, the level of success of that operation, and details on any operations that failed. Unlike the Credential Test feature, Collection Validation will not automatically add a credential entry or update an existing entry.

The Collection Validation process is run in the context of a particular credential entry, against a particular device. Once the Validate button has been selected, you will be asked to enter the IP address of a device that you would like to run the Validation process against. Make sure that the IP address you select corresponds to the proper type of device. For instance, if running Collection Validation from the Windows credential section, select a Windows Server or Workstation.

The process may take up to a couple of minutes to complete. The Discovery, Inventory, and Performance collection processes will be run against the selected IP address. These processes exactly match the operations that are run during the normal scanning and performance collection stages of the engagement, although the Collection Validation feature does not store any collected data and will not affect any aspect of the platform, such as Assets or reported performance analytics.

The validation process will start by confirming that the device will be discovered during a scan of the environment. This involves an ICMP Echo Request (ping) to determine if the device exists on the network, combined with a TCP/UDP port test to discover what protocols are available on the device. If an ICMP Echo Reply is not received, then the validation process will stop. Similarly, if the type of protocol associated with the type of credential being tested is not available, for instance if WMI (TCP 135) is not available when testing a Windows credential, then the validation process will stop, as it will not be able to communicate with the device.

Next, the Inventory process will run, which is responsible for collecting the data from the device that is shown in the Assets page. This may include data such as the Operating System type and version, network interfaces and addresses, disk storage, etc. The operations that collect this data will be logged, and the result of each collection operation will be shown. Details on the result codes are provided below. The Discovery process checks to see whether the relevant protocol is reported to be available, but the Inventory process tests the ability to communicate and authenticate with that device using the appropriate protocol. If communication or authentication fails, then the validation process will be stopped, and any available details on why the attempt failed will be displayed.

Finally, the Performance collection process will run. When a device is licensed for performance collection, this process is periodically run against that device for the duration of the performance collection period, typically as long as the device is licensed. Like the Inventory process, each operation that is issued to the device for data collection will be logged, along with the result of that operation.

Once the collection processes have finished, a report is then presented to provide the details of what operations were performed, the Result Code of each operation, an Overall Status describing how complete the collection activity was, and any available details for operations that did not complete successfully. See below for details on the Overall Status, and the failure details section. This report can also be copied into the clipboard, in case the report needs to be saved or copied to one of our support staff. In order to do this, the Text Version button should be selected, which displays the report as plain text, and then the Copy button should be selected to copy the text into your clipboard.
Overall Status

The Overall Status provides a high-level status of how complete the data collection activity was. The possible Overall Statuses, and their descriptions are:

Table 3-2 • Overall Status

<table>
<thead>
<tr>
<th>Overall Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>All collection operations completed successfully, and the device is fully prepared for participation in the engagement. No further action is required.</td>
</tr>
<tr>
<td>PARTIAL</td>
<td>Some non-critical operations did not complete successfully. The device is prepared for participation in the engagement, but some further action may be required to ensure the best possible data. Further action is at the user’s discretion.</td>
</tr>
<tr>
<td>FAIL</td>
<td>At least one critical operation failed. The device may not be prepared for participation in the engagement, or some critical data will not be</td>
</tr>
</tbody>
</table>

Result Codes

For each operation run during the validation process, what operation is performed and the result of that operation is logged. Understanding the result codes is the key to understanding the output of the Collection Validation feature.

All operations may result in the SUCCESS code, which indicates that the operation completed successfully and collected the associated data. Any other result code shows the manner in which the operation failed, in respect to the outcome of that failure.

Table 3-3 • Result Codes

<table>
<thead>
<tr>
<th>Result Code</th>
<th>Description</th>
<th>Overall Status</th>
<th>Cause for Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUCCESS</td>
<td>The operation was successful.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>FAIL</td>
<td>The operation failed, where either the collection attempt was not successful, or data was not returned. A FAIL code is always cause for concern and further action.</td>
<td>FAIL</td>
<td>Yes</td>
</tr>
<tr>
<td>EXPLORE</td>
<td>The operation failed, but the specific operation or the data it is intended to collect is not critical. Often, this indicates an operation that tests for the availability of some data or collection method.</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>FALLBACK</td>
<td>The operation failed, but a fallback operation to collect equivalent data will immediately follow. Used in cases where a preferred operation may not be available, and an alternative method is available.</td>
<td></td>
<td>Maybe (see below)</td>
</tr>
</tbody>
</table>
For these non-SUCCESS result codes, you should do the following:

- **FAIL**—Any operation that reports a FAIL result should be investigated and corrected. Under normal collection activity, this may prevent data collection activity for the device or critical data will be missing from the platform.

- **EXPLORE**—Operations that result in an EXPLORE status can be safely ignored. A failure from an EXPLORE operation will not negatively affect data collection, and is shown in the Collection Validation report for logging purposes.

- **INCOMPLETE**—Operations that result in INCOMPLETE may or may not be an issue, depending on what data is interesting in the context of a specific engagement. An operation related to critical data for the platform will never result in an INCOMPLETE. For instance, a failure to collect hardware platform information from a Linux/UNIX device using the SSH Collection Module is not critical for the core value of the platform, but in cases where this data is important for the goals of an engagement further action to correct the issue may be necessary.

- **FALLBACK**—The FALLBACK result warrants the most explanation. This is reported for an operation that failed, but another (typically less preferred) operation is available to be run immediately afterwards to attempt to collect equivalent data. This means that the operation that is logged immediately following one that reported a FALLBACK result will indicate whether further action is required. If a FALLBACK is immediately followed by a SUCCESS, then the second operation was successful and no further action is required. If a FALLBACK is immediately followed by a FAIL, then all attempts to collect particular critical data were exhausted, and the issue must be corrected. If a FALLBACK is immediately followed by an INCOMPLETE, then all attempts to collect particular non-critical data were exhausted, and further action to correct the issue is at the user’s discretion. Collection of particular data may have multiple fallback operations, so a FALLBACK may be immediately followed by another FALLBACK. Such a string of operations will always terminate with a result code other that FALLBACK, which indicates the ultimate outcome of the attempt to collect that data.
Chapter 3  Getting Started with Foundation and CloudScape
Discovery Troubleshooting

Failure Details

If any operations did not complete with a SUCCESS result code, further details on the operation are provided at the top of the report. The data is broken into sections for the Inventory and Performance collection processes, although some operations may be common to both components any may display twice in the report. The particular format of the data depends on the protocol in use, but generally will include the operation itself, the class of failure encountered, and any error messages or other output produced by the operation.

As an example using the SSH Collection Module, the output may be:

Table 3-4 • Error Message Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td>Command Failure</td>
</tr>
<tr>
<td>Result</td>
<td>FAIL</td>
</tr>
<tr>
<td>Command</td>
<td>sudo ifconfig -a</td>
</tr>
<tr>
<td>Exit Code</td>
<td>1</td>
</tr>
<tr>
<td>Standard Output</td>
<td></td>
</tr>
<tr>
<td>Standard Error</td>
<td>sudo: no tty present and no askpass program specified</td>
</tr>
</tbody>
</table>

In this case, the command ‘sudo ifconfig -a’ returned a non-zero exit status, indicating that the command did not complete successfully. As this command is critical for proper data collection, a failure from the command results in a FAIL result status, which in turn sets the Overall Status to FAIL as well. No output on the standard output stream (STDOUT) was produced, but the standard error stream (STDERR) produced the error message ‘sudo: no tty present and no askpass program specified’, indicating that sudo has not been properly configured to allow the command. Further action is required, in this case to review the sudo configuration to ensure that the ifconfig command is properly permitted, according to the SSH Collection Module documentation.
Common Issues Resulting In A PARTIAL Status

Some operations have a higher than normal likelihood of issues that cause an Overall Status of PARTIAL. Some of these errors are documented below, with the degree of severity and recommendations on how to resolve them.

Invalid Argument SSH Error

Table 3-5 • Invalid Argument SSH Error

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>cat /sys/class/net/eth0/speed</td>
</tr>
<tr>
<td>Error</td>
<td>cat: /sys/class/net/eth0/speed: Invalid argument</td>
</tr>
<tr>
<td>Result</td>
<td>INCOMPLETE</td>
</tr>
<tr>
<td>Description</td>
<td>The Linux kernel cannot report the speed of a network interface, in this case the eth0 interface. Typically this data is not available to Linux itself, which is usually seen with older kernels on virtualization environments</td>
</tr>
<tr>
<td>Recommendation</td>
<td>This issue does not currently have a resolution, so no action is required</td>
</tr>
</tbody>
</table>

No dmidecode SSH Error

Table 3-6 • No dmidecode SSH Error

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>which dmidecode</td>
</tr>
<tr>
<td>Error</td>
<td>which: no dmidecode in (/usr/local/bin:/usr/bin)</td>
</tr>
<tr>
<td>Result</td>
<td>INCOMPLETE</td>
</tr>
<tr>
<td>Description</td>
<td>This will typically follow the command /sys/devices/virtual/dmi/id, with a result of FALLBACK. Newer Linux kernels (2.6 and above) expose hardware platform data (hardware vendor, product, serial, etc) under the sysfs filesystem, which is the preferred approach for collection. When this is not available, the collection process checks for the availability of the dmidecode utility to collect the same data. This utility is typically not present in the default installation of most Linux distributions, so a failure to detect this utility as the fallback method will result in the exhaustion of the methods for collection that data, and an INCOMPLETE status.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>If hardware platform data is desired, which is shown in the Assets page, installing the dmidecode utility and making it available using sudo, as described in the SSH Collection Module documentation, will resolve this behavior.</td>
</tr>
</tbody>
</table>
Common Issues Resulting In An ERROR Status

The following are commonly seen issues that result in an ERROR status, and the potential for an inability to continue collection on a device.

Stale File Handle SSH Error

Table 3-7 • Stale File Handle SSH Error

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>df -P</td>
</tr>
<tr>
<td>Error</td>
<td>df: /some/mount/point: Stale file handle</td>
</tr>
<tr>
<td>Result</td>
<td>FAIL</td>
</tr>
<tr>
<td>Description</td>
<td>The df utility is used to collect the filesystems present on a Linux/UNIX device. In some cases, particularly related to NFS, the kernel thinks that a filesystem is mounted when it is not, or an NFS filesystem has been detached. According to the POSIX standards, the df utility will return a non-zero exit status on an error, which it does in this case. In order to ensure that all filesystems mounted on the system are properly accounted for, in the case that df returns an error it is considered a critical command failure.</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Investigate the system in question to determine why df is unable to report on certain filesystems, and fully mount or unmount the problematic filesystem. It may also be possible to cause the system’s cache of mounted filesystems to resync.</td>
</tr>
</tbody>
</table>

Protocol Specific Troubleshooting

For specifics on troubleshooting certain devices please proceed to the troubleshooting subsections of the following pages:

- Windows Collection Module
- SSH Collection Module
Discovery Help

If you have any questions or need further assistance that is not covered in the documentation then please open a ticket with our support team. When opening a ticket regarding devices not being discovered, the following information is required:

- **Windows Devices**
- **Linux Devices**

**Windows Devices**

Information required for Windows devices.

**Table 3-8 • Information Required to Create a Ticket for Windows Devices**

<table>
<thead>
<tr>
<th>From Host</th>
<th>Result</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Host</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Information</td>
<td></td>
<td><code>ipconfig /all</code></td>
</tr>
<tr>
<td>Firewall Information</td>
<td></td>
<td>Screenshot of windows firewall status</td>
</tr>
<tr>
<td>WBEM Test local</td>
<td></td>
<td>How to use <code>wbemtest.exe</code> to validate Windows Credentials:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Video</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>wbemtest.exe</code> doc</td>
</tr>
<tr>
<td>Service List</td>
<td>Screenshot of all services that are running (for 3rd party firewall check)</td>
<td></td>
</tr>
<tr>
<td>Source Host</td>
<td>IP Information</td>
<td><code>ipconfig /all</code></td>
</tr>
<tr>
<td>Note • Some other box on the customer's network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note • This box should be on the same subnet as the RN150</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping to Target host</td>
<td></td>
<td><code>ping x.x.x.x</code></td>
</tr>
<tr>
<td>WBEM Test Remote</td>
<td>How to use <code>wbemtest.exe</code> to validate Windows Credentials:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>wbemtest.exe</code> doc</td>
<td></td>
</tr>
</tbody>
</table>
### Linux Devices

Information required for Linux devices:

**Table 3-9 • Information Required to Create a Ticket for Linux Devices**

<table>
<thead>
<tr>
<th>From Host</th>
<th>Result</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target Host</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Information</td>
<td>ifconfig -a</td>
</tr>
<tr>
<td></td>
<td>Firewall Information</td>
<td>sudo iptables -L -n</td>
</tr>
<tr>
<td><strong>Source Host</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Information</td>
<td>ifconfig -a</td>
</tr>
<tr>
<td>Note • Some other box on the customer's network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note • This box should be on the same subnet as the RN150</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping to Target host</td>
<td>ping x.x.x.x</td>
<td></td>
</tr>
</tbody>
</table>
| SNMP Walk of All MIBS | | UCD: snmpwalk -v2c -cstring x.x.x.x ucdavis
  | | UCD-DISKIO: snmpwalk -v2c -cstring x.x.x.x ucddiskiomib
  | | HOST-RESOURCES: snmpwalk -v2c -cstring x.x.x.x host
  | | TCP: snmpwalk -v2c -cstring x.x.x.x tcp
  | | IF: snmpwalk -v2c -cstring x.x.x.x interfaces |
This section provides you with instructions on how to operate, interpret, and utilize the platform after the Discovery and Inventory phases are successfully completed.

- Building Application Stacks
- Mapping Applications
- Reports/Pages
- Glossary
- RESTful API Access
- RN150 Migration

### Building Application Stacks

Information about building application stacks is described in the following sections:

- Application Stacks Overview
- Part One: Build Application Stacks
- Part Two: Verifying Scope with RSG-Out of Scope Services
- Part Three: Application Stack Review and Refinement

### Application Stacks Overview

One of the primary goals for a discovery project is to organize all of the discovered (and licensed) workloads into the various Application Stacks that they support. Once this organizational work has been completed, the platform is better positioned to provide dependency, cloud costing, resource requirements, and other information from an application-centric point of view. This view supports more detailed planning and analysis for Strategic IT Planning, Cloud and Data-center migration, Security reviews, CMDB updates, and other use cases.
Building Application Stacks is the process of reviewing and refining the automatically generated application stacks (AutoApp_XXX), taking system dependencies, input from application teams, best practices, and other factors into account. There is not necessarily one way to approach this process, however this document will outline some best practices for application review and refinement. The end result of this effort should be a set of application stacks that most closely represent the source environment and provide the vantage point needed to support the desired outcome(s).

- **How Are App Stacks Built?**
- **How to View Connectivity**

**How Are App Stacks Built?**

The Foundation and CloudScape platform joins servers into groups based on the collected connectivity and process information. There are different group types the platform will create automatically whose definitions can be found on our Glossary page under the subsection “Group Definitions”

**How to View Connectivity**

All of the processes outlined below are completed using the following two pages of the portal:

- **Add Intelligence >> All Applications**
- **Add Intelligence >> View Individual Application Stacks**

Connectivity can be visualized by working in and expanding the right side frame on both of these pages. This includes providing the ability to visualize critical or all connectivity as well as viewing connectivity internal to the application stack, external to the application stack, or both (all). When viewing the **Add Intelligence >> View Individual Application Stacks** page you also have two additional options for viewing and navigating connectivity information:

- **View All Connections (top left)**—Provides a table summary of all connectivity and includes three levels of drill down
- **Dependent Stacks (from visualization control)**—Provides a visualization of all stack-to-stack connectivity relative to the individual stack you are currently viewing.

**Tip** • The View All Connections can be an important way to view connectivity because it is NOT limited to connectivity between licensed nodes. The visualizations are limited to connectivity between licensed nodes with the exception of the RSG-Out Of Scope Services group.

**Tip** • In any visualization you can click on a line segment to view the details specific to that relationship whether it be workload to workload, or application stack to application stack.

**Part One: Build Application Stacks**

Once a sufficient amount of connectivity data has been collected in the environment the select the **Build App Stacks** button in the top left of the **Add Intelligence >> All Applications** page. This will kick-off the RISC Networks Intelligent Application Grouping Algorithm. Which will cause servers to be joined into groups based on their connectivity.

For more information, see **Group Definitions**.
Part Two: Verifying Scope with RSG-Out of Scope Services

The initial and primary mechanism of setting the scope for is the discovery phase (as described in How We Collect). During this phase you will select the subnets to include in discovery and ensure you have access to the workloads contained within the boundaries of those subnets. However, additional scope validation can be performed post-licensing through a review of a special auto-generated application stack called RSG-Out Of Scope Services.

The following includes the steps needed for a detailed review of the RSG-Out Of Scope Services group. The level to which you will need to perform this is dependent on the need for true “discovery” of the environment. In other words, if you are leveraging the discovery aspects of the platform to find systems you may not know about or have documentation on, then you would perform this validation in detail. If you are running the Foundation and CloudScape platform against a known subset of the environment, then a more cursory review of RSG-Out Of Scope Services may be sufficient.

- Step One: Verify Whether Hosts Should Be Brought Into Licensing/Scope
- Step Two: Make Sure There Are No Unlicensed Consumers
- Step Three: Verify Whether the Out-of-Scope IPs Should BeLicensed

**Step One: Verify Whether Hosts Should Be Brought Into Licensing/Scope**

Iterate through the RSG-Out Of Scope Services group and verify whether or not the hosts in this group should be brought into licensing/scope. Our default advice is that everything in the environment should be licensed during the burst, so working through this group can be an important first step in ensure a complete scope.

Once you license the devices in the RSG-Out Of Scope Services group (or decide that they are to remain out of scope), you should re-run auto-grouping to make sure that the group is empty – or that all hosts can be safely ignored.

**Caution • You should routinely re-run auto-grouping and check this group as new services may come online at any time.**

**Step Two: Make Sure There Are No Unlicensed Consumers**

Make sure that there are not any CONSUMERS of services that are not licensed. This means going through the individual application stacks and checking their connectivity to “locations”. For specific definitions of locations please refer to our Glossary under the subsection Connectivity Definitions.

To check consumption of important services, click View All Connections when viewing the RSG-Out Of Scope Services stack. This will bring up a table of all group- to-group and group-to-location connectivity. Sort this table by the destination group such that the RSG-Out Of Scope Services group is the destination. Once sorted, on the far right of the table you will see a “View Details” link, you should click this link for the first location listed in the source column. This will bring up another table that you should then click the button in the top left of the table to show a protocol view. Review the listed protocols to understand connectivity and if there are important services being consumed outside of this group. You want to verify that the traffic is not on a well-known port or protocol name, such as MSSQL, oracle, MySQL, etc… To understand
particular IPs that are communicating on a protocol select the “View Details” link on the far right of the table, this will bring up another table that lists out the specific IP addresses. You should verify this list to understand if those items currently not licensed should be brought into scope. Repeat these steps for every location group within the first group to group/location table.

Tip • If you have a large environment where going through all the AutoApp stacks would be too time consuming, then the best way to determine consumers of services out of scope is to run the auto-grouping with the 95th group and view this information against the RSG-95th Highly Connected Stack. The RSG-95th Highly Connected Stack is the top 5% of hosts by connectivity in the network. In other words, it is the list of servers that talk the MOST. The “hosts with the most” we like to say.

Step Three: Verify Whether the Out-of-Scope IPs Should Be Licensed
Verify whether or not the out of scope IPs that are CONSUMERs or are OFFERING important services described above should be licensed. The group of the service host (the one offering the service) is inconsequential. The important thing is to determine if all of those hosts should be brought into scope and licensed as they may be front end servers or other applications that are accessing servers you are focused on. Once this process has been repeated, and there are not major connections in or out of the 3 major groups (Isolated Devices, RSG-95th Highly Connected Stack, and RSG-Out Of Scope Services), you can move on to application review.

Part Three: Application Stack Review and Refinement
Information about application stack review and refinement is described in the following sections:
- Application Stack Review and Refinement Overview
- 95th Resolution Approach
- Visualization and Movement Approach
- Review for Critical Dependencies

Application Stack Review and Refinement Overview
First, it is important to understand what your starting or initial reference point will be. For most organizations, this will be the set of Application Stacks that are automatically generated by the platform using the Build App Stack function (found in Add Intelligence >> All Applications).

Some organizations may prefer to use internally documented Application-to-Server mappings as the baseline to begin this process (e.g. CMDB). In this case the Application Stacks must be manually created and workloads are assigned to them as documented.

The Foundation and CloudScape platform has several UI features that allow for bulk manipulation of server workloads and their assignment to specific application stacks. This includes the ability to filter server lists based on naming convention, shift select, and right click to assign to an existing or new Application Stack.

No matter which methodology you use as your initial reference point, you will likely use a combination of connectivity data, internal documentation (CMDB), and “tribal knowledge” during the Application Review and Refinement process.
Tip • Use the Graph in Add Intelligence >> All Applications to switch the view from Application Stacks to servers. You can sort and filter on any column in order to facilitate bulk movement of workloads to Application Stacks. Since Application Stack is one of the available columns this can also help to locate systems in the platform.

There are two techniques that can be used to review and refine automatically generated Application Stacks: 95th Resolution and Visualization with Movement. We recommend having the application owners participate in either approach as they can more rapidly iterate over known hosts based on their knowledge of the environment.

Tip • The easy way to determine which approach would work best for you is to first Build App Stacks without the 95th group. This will, generally, generate several application stack groups (AutoApp-xxx). Review these groups by selecting them and viewing the number of hosts in a group. If a group appears to have over 50 hosts, then visualize the group. This will visualize connectivity for that group, if the visualization is unworkable from either a portal performance perspective or visually because there are too many connections then you should proceed with the 95th Resolution approach, otherwise the initial auto-grouping was sufficient and you can continue with the Visualization with Movement approach.

Tip • There is a filter by number of connections slider within the left slide out on the visualization that can be used to determine highly connected servers easily within large visualizations

Tip • Before you begin creating your own application stacks it is important to come up with a good prefix and suffix structure to “tag” application. This will be very useful when looking at subsequent reports and visualizations. (e.g. ITM-XXXX-PRD would be an IT management app in my production environment vs. BUS-XXXX-DEV would be a business application in my development environment.

95th Resolution Approach

This approach utilizes the RSG-95th Highly Connected Stack. By running the auto-generation of application stacks with the 95th Percentile option selected, you will generate a group called RSG-95th Highly Connected Stack – which will be a small subset of heavily connected nodes.

• Step One: Review and Disposition Each Host in the 95th Group
• Step Two: Create a New Application Stack
• Step Three: Re-Run the Auto Generate Groups Algorithm Without the 95th Group

Step One: Review and Disposition Each Host in the 95th Group

Review and disposition each host in the 95th Group… “What is this host used for?”. Typically, you will have knowledge of these hosts since they are so heavily connected. You should disposition each host within the group into one of two categories:

• Services—These would be hosts that are offering a service to the rest of your environment. We have attempted to capture some of these in our RISC Service Group(s) such as exchange, Citrix, NFS, etc, but we have not scripted for every service that can be offered. Something like antivirus, authentication, logging, etc. would be examples of services. To disposition a Service, create a new application stack (antivirus for example). Once this is complete move that host by right clicking the host and selecting Edit Stack Membership.
Chapter 4  Using the Platform
Building Application Stacks

- **Application Stacks**—These would be hosts that are a part of an application stack. These could be things like a shared DB. There are two ways to disposition a member of an application stack. For environments with heavily shared architectures (think large jboss layers or large shared DBs) proceed to Step Two, otherwise disposition Application Stacks by simply leaving them in the 95th Group and proceeding to step two.

**Step Two: Create a New Application Stack**

**Important** • This is only for environments with heavily shared architectures as noted above; otherwise skip this step.

Create a new application stack (Shared DB for example). Move the server(s) that are part of that cluster (or it might just be a single db server) into the new application stack you just created.

You can immediately view the connections of that application stack and see where that server or cluster is communicating. You would likely see other AutoApp-xxx stacks. If this communication is important (such as DB traffic), it is an indication that these application stacks are likely front ends running off of the DB. If the DB is shared, you can leave it there, and rename the front end groups (e.g. AutoApp-xxx becomes Main SAP FrontEnd) or you can move the servers from AutoApp-xxx into the new group you built for the server(s) you pulled from the 95th group.

You repeat this process until the 95th group is empty. If you want to do a second round, you can re-run the auto-grouping and select the 95th group again. Since the original top 5% were grouped into Application Stacks, a new set of top 5% hosts will be identified and included in the 95th group, and can now be rationalized and grouped using the same methods as above.

This is a very effective approach in environments with heavily shared architectures (think large jboss layers or shared DBs)

**Step Three: Re-Run the Auto Generate Groups Algorithm Without the 95th Group**

Re-run the Auto Generate Groups algorithm without the 95th group. This will place any remaining workloads, not in a saved or confirmed Application Stack, into an AutoApp_XXX stack based on connectivity. Proceed to the Visualization and Movement Approach.

**Note** • Any application stacks not saved or confirmed upon re-execution of the algorithm will be deleted and rebuilt. Only those Application Stacks that have been saved or confirmed will remain intact.

**Visualization and Movement Approach**

This approach works well in environments that are not heavily shared (no large DB farms or jboss/tomcat layers). We recommend having the application owners participate in this process as they can more rapidly disposition hosts based on their knowledge of the environment.

Run auto-grouping without the 95th group. This can sometimes result in large vertical stacks that may join together multiple stacks if they use a shared resource or an unmapped RSG (an infrastructure service that we have not identified yet).

Once you begin to go through AutoApp-xxx stacks, you can visualize them. In many cases you will see a single server or a small group of servers that link all of the hosts together. You can use the table below the visualization to see the actual application processes in use on the connections (if netstat data was collected).
Our auto generated groupings may group single applications or multiple if they share DBs for example. Your objective is to decide how to and if application stacks should be broken into smaller ones. You can then make a decision as to whether that host (or small group of hosts) should be allowed to link those groups together. (We have already decided YES, but you can overrule us!) If not, right click on the host, select Edit Stack Membership and create a new application stack to move the host into. You can then immediately close the visualization and re-open it, to see the result of your move.

The visualization may now show multiple clusters of servers. What you are seeing is the result that you will get the NEXT time you run Build App Stacks. You must re-run the auto-grouping to have the system break that stack apart, into two or more application stacks.

Once this has been completed you should disposition that group by giving it a friendly name that is meaningful to you and the business (e.g. AutoApp-xxx should be renamed to ApplicationName).

Repeat this process for each AutoApp_XXX Application Stack. All of this should be done with the application owners input. So while you may iterate a few times before you engage the application owner(s), they are critical to making the ultimate decisions on validating groups.

**Tip •** Remember to view connectivity data to check the inter-stack relationships and make sure that there are not any critical dependencies that would require further investigation or stack membership changes. This is also where you can check and verify that you don’t have unlicensed hosts using a service on a licensed node.

### Review for Critical Dependencies

Once you have refined and confirmed an Application Stack, it is important to review the connectivity data for critical dependencies. These are dependencies that would dictate a change in Application Stack membership (e.g. a workload that needs to be moved into the stack you are reviewing).

For instances where there is connectivity that is critical and noteworthy but does not dictate a change in stack membership, you may choose to document this information for planning purposes. This can include Reporting, BI, or Data Transformation services that leverage database connectivity into these Application Stacks. There are several options available to view connectivity for this purpose:

- **Workload Based Visualizations**
- **Application Stack Based Visualizations**
- **View All Connections**

### Workload Based Visualizations

When you select an Application Stack in Add Intelligence >> All Applications or when you are in the View Individual Application Stack view, the bottom right hand section of the page provides a workload based visualization. Expand the visualization to provide more working area and use the visualization controls to show All connectivity that is Critical.

This provides an easy way to see workload to workload connectivity. You can click on any segment to view the details specific to that relationship. Make sure to use the column chooser to make sure you include application and process information. Review the connectivity to determine if any of it requires a change in Application Stack membership or if something that is noteworthy and must be somehow accounted for in your migration plan.
Tip • You are typically looking for “critical” connectivity such as Oracle, MySQL, MSSQL or known application traffic such as SAP.

Application Stack Based Visualizations

When viewing the Add Intelligence >> View Individual Application Stacks page, you have the option to view Dependent Stacks (from visualization control). This provides a visualization of all stack-to-stack connectivity relative to the individual stack you are currently viewing. Use the visualization controls to filter out infrastructure services such as Active Directory, Antivirus, etc. This allows you to focus on true application to application connectivity.

From here you can select any Application Stack to Application Stack segment that is interesting or that requires further investigation. By default, this will return a listing of the host to host connectivity that exists between these two stacks.

You can switch this to a Protocol view to review from this basis. Again you are typically looking for “critical” connectivity such as Oracle, MySQL, MSSQL or known application traffic such as SAP. If you do see a protocol that is critical or interesting, you can View Details to drill into this and see the specific host to host connectivity for this protocol. This will also list the application and processes associated with the connectivity adding additional context to your review.

Continue reviewing these Application Stack to Application Stack relationships until you are satisfied that there is nothing that would dictate a change in Application Stack membership.

View All Connections

When viewing the Add Intelligence >> View Individual Application Stacks page you have the option to View All Connections (top left). This provides a table summary of all connectivity specific to that Application Stack and includes three levels of drill down.

The View All Connections option can be an important way to view connectivity because it is NOT limited to connectivity between licensed nodes. The visualizations are limited to connectivity between licensed nodes with the exception of the RSG-Out Of Scope Services group. Use this option to view connectivity coming into or out of the licensed environment.

For example, you can use this dialog to determine if an Application Stack is Internet facing. In this case you will see connectivity coming in from the RISC-unknown-internet location.

Mapping Applications

You may have noticed lists of running processes, installed applications, and weird terms like “application context”. This document will explain how the product maps running processes to higher level software/applications installed. The process is similar for both Linux and Windows devices.

• Definitions
• Available Reports
• The Mapping Process

Definitions
The following are definitions:

- **Application Context**—This is the application we have mapped a process to be running within. For Linux devices (Generic Servers) we also include the description of the application in parenthesis in this field. This corresponds to src and dest app context in connectivity data AND Application Group on the Search Applications & Processes page.

  **Tip** • If you search for a context of installed you will see which applications were pulled from the registry

- **Name**—The executable that has been stripped of the command line information. This corresponds to src and dest app name in connectivity data AND Application Name on the Search Applications & Processes page.

- **Instance**—We can pull the custom name of the application from the command line of a few applications (e.g. Microsoft IIS).

- **Version**—This is the version of the application collected from the registry. This will display as unknown if we are not able to successfully map the running process to the registry.

### Available Reports

This data is available for reporting and exploration in several areas, the main ones are:

- **Assets**—When clicking to view the details of an individual device you will see a table reporting on these areas.

- **Device Details**—This is specific to an individual device and can be found through either right-clicking a device on a visualization or visiting the page directly.

- **Search Applications & Processes**—This page is useful for doing broad searching across the environment. You can search for either servers that match the search term or the specific application data that matches

- **ApplicationStackProcess**—This report is available in the “Available Reports” section. This is the best report for a consolidated export of all collected application data. You also have more filtering functionality within this report

### The Mapping Process

To perform the mapping process, perform the following steps.

**Task** • To perform the mapping process:

1. Pull registry (or rpm) of installed programs from system. The key fields pulled for this purpose are install path and display name.

   **Note** • All installed applications pulled from the registry will have the application context of “installed”.

2. Collect running processes.

3. Perform a fuzzy match on the file path of the running process to the install path of the installed applications. If a match is found to a certain degree of confidence then map the display name pulled from the registry to the application context.

4. If 3 fails (as not all entries in the registry have install paths or not all applications are in the registry), perform a fuzzy match on the display name into the file path of the running process. If a match is found to a certain degree of confidence then map the display name pulled from the registry to the application context.
5. If 4 fails then fall back to an internally curated database of regular expressions for associations
6. If 5 fails then label the context as “unknown”

Tip • If we successfully mapped back to the registry for Windows devices the Application Name will have “.exe” appended or for Linux devices the description pulled from the rpm will be in Application Context

Reports/Pages

The platform offers many reports and pages for you to use and gain actionable information from. Select one of the reports on the right to view its associated documentation.

- Assets (Legacy)
- IaaS Cloud Pricing
- Subscription Administration
- Visualize Topology
- Total Cost of Ownership
- Geolocation
- Assets & Asset Errors
- Threats
- Optimization Scorecard

Assets (Legacy)

The Assets page (located underneath Consume Intelligence > Assets) of the platform is meant to be your working page for reviewing the discovery results and taking further action. The Assets page is meant to be a listing of devices discovered within the customer environment. It should be used in an iterative process for scope setting/discovery of the customer’s environment (i.e. it is used as a working document throughout multiple scans to troubleshoot and discover further areas of a customer’s environment until the target scope is achieved).

Review How We Collect to gain a more in-depth understanding of the discovery process/what the appliance is doing.

The Asset Report is generated after the RN150 has completed the inventory phase. The appliance/assessment always works in this manner:

The Asset Report lists all devices that responded to an ICMP ping. Additionally, if we were able to connect to them using the provided credentials and categorize them they are further classified into device types (e.g. Windows Server, Windows Workstation, etc), as described in Device Type Definitions. Each category in the Asset Report aligns to a specific credential input into the appliance. (i.e. Devices under the Windows Server link indicate we have WMI access to that box, the Linux/Unix link shows SNMP or SSH accessible devices, if it is in the Virtual Machine link we have vCenter access, etc.). Clicking each link will filter the table below to show just those devices.
Key Takeaways

- **The report is additive.** With each successive rescan of the environment the newly discovered data will be added to that of the previous scan. Data is never removed, even in the event that credentials or subnets are removed or deselected for scanning in the appliance.

- **There is often overlap between the links.** Since they correspond to a credential we could have a Windows VM that is in both the Windows link and the VM link as it responded to both sets of credentials (Windows Admin and vCenter). Additionally, it can be in the inaccessible devices link if one credential worked, but not another (e.g. vCenter passed, but Windows failed). Please note that the Foundation and CloudScape platform will resolve the duplicate devices when doing subsequent reporting (you will only see one device for the VM and Windows Server), but the asset report is purposefully left as-is so that virtual teams and windows teams can both confirm the expected asset list.

IaaS Cloud Pricing

IaaS cloud pricing is described in the following sections:

- **About Cloud Pricing**
- **Instance Matching**
- **Supported Cloud Providers**
- **Cloud Pricing Values**

About Cloud Pricing

The IaaS Cloud Pricing feature simplifies the process of pricing and comparing cloud providers by determining the instance types that best fit the workloads in the environment, and the base costs associated with those instances.

Instance Matching

The core functionality of the IaaS Cloud Pricing feature is its ability to determine which instance type for a given provider best fits a system. There are two types of instance matches, based on differing data, inventory and usage.

- **Inventory matching** compares the resources present and usable (provisioned) by the device against the various cloud instances, to provide a match on what is already present in the environment. However, many systems may not be utilizing the full potential of the hardware.

- **Usage matching** determines the instance type that is the best fit for the actual workload (performance) of the system, based on the data collected during the performance collection period of the assessment.

Instance matching is based solely on CPU and memory, so storage pricing is not a component of which instance a device best matches. Currently, storage cost is based on inventory data, so the inventory and usage matching will be the same. Instances typically include some storage built into the virtual machine for use as the root volume of the system, and is included in the base cost of the instance.

Storage Metrics

When calculating the storage cost for a device for a given provider, any storage included in the instance is deducted from a system's reported storage prior to calculating the cost. For instance, if a system has 200 GB of storage and matches an instance with 40 GB of included storage, storage cost is calculated for 160 GB.

The quantity of storage calculated for a system is the summation of all locally attached storage, using the total size of each volume rather than utilized storage, from which any included instance storage is subtracted as explained above.
The Storage Cost field of the IaaS Cloud Pricing page reports the cost per hour.

**Network IO**

There are two types of network IO:

- **No flow data being collected**—By default (no flow data is being collected), we calculate the total bytes that each server sends (by watching its network interfaces through polling) in a given month and then apply the cloud provider's cost to that number for a month. We then divide back to get the cost per hour. This assumes that ALL traffic leaving any server's interface is charged traffic.

  So traffic between two servers in a stack will be counted even though it will not wind up being charged once migrated. Our Network costs are considered “worst case” scenarios. If you capture flow data, however, then we ARE able to discern which traffic leaves the stack and to which other stacks (infra services, on premise dbs, etc) it goes. You can then model the true network cost based on what you are migrating at any given point.

- **Netflow (Flow) data being collected**—If Netflow (Flow) data is collected – this enables us to see the source and destination of traffic on the wire and we can then model the network cost more accurately. There is a separate report that is generated to provide this analysis – so that you can model it in different ways and it can be requested via support.

The CloudScape platform field named **Instance Cost** reports the base cost of the matched instance.

**Supported Cloud Providers**

The following are the supported cloud providers:

- Amazon AWS
- Microsoft Azure
- Google Cloud Platform
- Rackspace
- Softlayer
- Quest Technology Management

**Cloud Pricing Values**

The following is a list of the information generated by the CloudScape cloud pricing module and reported to the user for each server for both inventory and usage based matching.

- CPU Calculation
- Memory Calculation
- Storage
- Storage IO
- Network IO
- Total Daily Cost

For more information, see **Cloud Pricing Change Log**.
Cloud Pricing Change Log

The following is the cloud pricing change log by cloud provider:

- Azure Updates / March 29, 2021
- Google Cloud Platform Updates / January 27, 2021
- AWS Updates / October 27, 2020
- Azure Updates / October 27, 2020
- AWS Updates / April 1, 2020
- Azure Updates / April 1, 2020
- Agilisys Updates / August 22, 2019
- AWS Updates / March 4, 2019
- Azure Updates / March 4, 2019
- AWS Updates / January 3, 2019
- Azure Updates / January 3, 2019
- AWS Updates / November 21, 2018
- Azure Updates / November 21, 2018
- AWS Updates / October 2, 2018
- Azure Updates / October 2, 2018
- AWS Updates / August 23, 2018
- Azure Updates / August 23, 2018
- AWS Updates / May 31, 2018
- Azure Updates / May 31, 2018
- AWS Updates / March 22, 2018
- Azure Updates / March 1, 2018
- Azure Updates / January 22, 2018
- Azure Updates / December 7, 2017
- Azure Updates / November 1, 2017
- Azure Updates / August 11, 2017
- Azure Updates / July 17, 2017
- Azure Updates / July 12, 2017
- Azure Updates / June 8, 2017
- Azure Updates / May 8, 2017
- Azure Updates / April 27, 2017
• Azure Updates / April 5, 2017

Azure Updates / March 29, 2021

• New Locations
• New / Updated Instances

New Locations
Brazil Southeast
Germany North (Public)
Germany West Central
Norway East
Norway West
South Africa North
South Africa West
Switzerland North
Switzerland West
UAE Central
UAE North

New / Updated Instances
Download the following CSV files:
AzureNewInstances29March2021.csv
AzureUpdatedInstances29March2021.csv

Google Cloud Platform Updates / January 27, 2021

• New Locations
• New Instances

New Locations
Google Cloud Platform - US Central 1
Google Cloud Platform - US West 1
Google Cloud Platform - US West 2
Google Cloud Platform - US West 3
Google Cloud Platform - US West 4
Google Cloud Platform - US East 4
Google Cloud Platform - US East 1
Google Cloud Platform - northamerica-northeast1
Google Cloud Platform - southamerica-east1
Google Cloud Platform - Europe West 1
Google Cloud Platform - Europe North 1
Google Cloud Platform - Europe West 3
Google Cloud Platform - Europe West 2
Google Cloud Platform - Europe West 4
Google Cloud Platform - Europe West 6
Google Cloud Platform - Asia South 1
Google Cloud Platform - Asia Southeast 1
Google Cloud Platform - Australia Southeast 1
New Instances

Iowa (us-central1), e2-standard series
Oregon (us-west1), e2-standard series
Los Angeles (us-west2), e2-standard series
Salt Lake City (us-west3), e2-standard series
Las Vegas (us-west4), e2-standard series
Northern Virginia (us-east4), e2-standard series
South Carolina (us-east1), e2-standard series
Montréal (northamerica-northeast1), e2-standard series
São Paulo (southamerica-east), e2-standard series
Belgium (europe-west1), e2-standard series
Finland (europe-north1), e2-standard series
Frankfurt (europe-west3), e2-standard series
London (europe-west2), e2-standard series
Netherlands (europe-west4), e2-standard series
Zürich (europe-west6), e2-standard series
Mumbai (asia-south1), e2-standard series
Singapore (asia-southeast1), e2-standard series
Sydney (australia-southeast1), e2-standard series

AWS Updates / October 27, 2020

- New Locations
- New / Updated Instances

New Locations

EU Milan
Africa Cape Town
US West Los Angeles
Middle East Bahrain
Asia Pacific Hong Kong
Asia Pacific Osaka 1 Year Reserved
Asia Pacific Osaka 3 Year Reserved
EU Milan 1 Year Reserved
EU Milan 3 Year Reserved
Africa Cape Town 1 Year Reserved
Africa Cape Town 3 Year Reserved
US West Los Angeles 1 Year Reserved
US West Los Angeles 3 Year Reserved

New / Updated Instances

Download the following text file:

Amazon Web Services (AWS): New / Updated Instances (October 27, 2020)

Azure Updates / October 27, 2020

- New Locations
- New / Updated Instances

New Locations

Brazil Southeast
Brazil Southeast 1 Year Reserved
Brazil Southeast 3 Year Reserved
Germany North
Germany North 1 Year Reserved
Germany North 3 Year Reserved
Germany West Central
Germany West Central 1 Year Reserved
Germany West Central 3 Year Reserved
Norway East
Norway East 1 Year Reserved
Norway East 3 Year Reserved
Norway West
Norway West 1 Year Reserved
Norway West 3 Year Reserved
South Africa North
South Africa North 1 Year Reserved
South Africa North 3 Year Reserved
South Africa West
South Africa West 1 Year Reserved
South Africa West 3 Year Reserved
Switzerland North
Switzerland North 1 Year Reserved
Switzerland North 3 Year Reserved
Switzerland West
Switzerland West 1 Year Reserved
Switzerland West 3 Year Reserved
UAE Central
UAE Central 1 Year Reserved
UAE Central 3 Year Reserved
UAE North
UAE North 1 Year Reserved
UAE North 3 Year Reserved

New / Updated Instances

Download the following text file:

Azure: New / Updated Instances (October 27, 2020)

AWS Updates / April 1, 2020

- New Locations
- New Instances
- Updated Instances

New Locations

US East 1 Year Reserved
US East 3 Year Reserved
US East Ohio 1 Year Reserved
US East Ohio 3 Year Reserved
US West Oregon 1 Year Reserved
US West Oregon 3 Year Reserved
US West Northern California 1 Year Reserved
US West Northern California 3 Year Reserved
Asia Pacific Hong Kong 1 Year Reserved
Asia Pacific Hong Kong 3 Year Reserved
Asia Pacific Mumbai 1 Year Reserved
Asia Pacific Mumbai 3 Year Reserved
Asia Pacific Seoul 1 Year Reserved
Asia Pacific Seoul 3 Year Reserved
Asia Pacific Singapore 1 Year Reserved
Asia Pacific Singapore 3 Year Reserved
Asia Pacific Sydney 1 Year Reserved
Asia Pacific Sydney 3 Year Reserved
Asia Pacific Tokyo 1 Year Reserved
Asia Pacific Tokyo 3 Year Reserved
Canada Central 1 Year Reserved
Canada Central 3 Year Reserved
EU Frankfurt 1 Year Reserved
EU Frankfurt 3 Year Reserved
EU Ireland 1 Year Reserved
EU Ireland 3 Year Reserved
EU London 1 Year Reserved
EU London 3 Year Reserved
EU Paris 1 Year Reserved
EU Paris 3 Year Reserved
EU Stockholm 1 Year Reserved
EU Stockholm 3 Year Reserved
Middle East Bahrain 1 Year Reserved
Middle East Bahrain 3 Year Reserved
South America Sao Paulo 1 Year Reserved
South America Sao Paulo 3 Year Reserved
GovCloud US East 1 Year Reserved
GovCloud US East 3 Year Reserved
GovCloud US West 1 Year Reserved
GovCloud US West 3 Year Reserved

New Instances
Asia Mumbai a1 series
Asia Mumbai g4dn series
Asia Mumbai i3en series
Asia Mumbai m4 series
Asia Mumbai m5 series
Asia Mumbai m5a series
Asia Mumbai m5ad series
Asia Mumbai m5d series
Asia Mumbai r5a series
Asia Mumbai r5ad series
Asia Mumbai x1e series
Asia Mumbai x1d series
Asia Pacific Hong Kong 1 Year Reserved c5 series
Asia Pacific Hong Kong 1 Year Reserved c5d series
Asia Pacific Hong Kong 1 Year Reserved d2 series
Asia Pacific Hong Kong 1 Year Reserved g4dn series
Asia Pacific Hong Kong 1 Year Reserved i3 series
Asia Pacific Hong Kong 1 Year Reserved m5 series
Asia Pacific Hong Kong 1 Year Reserved m5d series
Asia Pacific Hong Kong 1 Year Reserved r5 series
Asia Pacific Hong Kong 1 Year Reserved r5d series
Asia Pacific Hong Kong 1 Year Reserved x1 series
Asia Pacific Hong Kong 3 Year Reserved c5 series
Asia Pacific Hong Kong 3 Year Reserved c5d series
Asia Pacific Hong Kong 3 Year Reserved d2 series
Asia Pacific Hong Kong 3 Year Reserved g4dn series
Asia Pacific Hong Kong 3 Year Reserved i3 series
Asia Pacific Hong Kong 3 Year Reserved m5 series
Asia Pacific Hong Kong 3 Year Reserved m5d series
Asia Pacific Hong Kong 3 Year Reserved r5 series
Asia Pacific Hong Kong 3 Year Reserved r5d series
Asia Pacific Hong Kong 3 Year Reserved x1 series
Asia Pacific Mumbai 1 Year Reserved a1 series
Asia Pacific Mumbai 1 Year Reserved g4dn series
Asia Pacific Mumbai 1 Year Reserved i3en series
Asia Pacific Mumbai 1 Year Reserved m4 series
Asia Pacific Mumbai 1 Year Reserved m5 series
Asia Pacific Mumbai 1 Year Reserved m5a series
Asia Pacific Mumbai 1 Year Reserved m5ad series
Asia Pacific Mumbai 1 Year Reserved m5d series
Asia Pacific Mumbai 1 Year Reserved r5a series
Asia Pacific Mumbai 1 Year Reserved r5ad series
Asia Pacific Mumbai 1 Year Reserved x1e series
Asia Pacific Mumbai 3 Year Reserved a1 series
Asia Pacific Mumbai 3 Year Reserved g4dn series
Asia Pacific Mumbai 3 Year Reserved i3en series
Asia Pacific Mumbai 3 Year Reserved m4 series
Asia Pacific Mumbai 3 Year Reserved m5 series
Asia Pacific Mumbai 3 Year Reserved m5a series
Asia Pacific Mumbai 3 Year Reserved m5ad series
Asia Pacific Mumbai 3 Year Reserved m5d series
Asia Pacific Mumbai 3 Year Reserved r5a series
Asia Pacific Mumbai 3 Year Reserved r5ad series
Asia Pacific Mumbai 3 Year Reserved x1e series
Asia Pacific Mumbai 3 Year Reserved z1d series
Asia Pacific Seoul 1 Year Reserved c5 series
Asia Pacific Seoul 1 Year Reserved c5d series
Asia Pacific Seoul 1 Year Reserved g4dn series
Asia Pacific Seoul 1 Year Reserved m4 series
Asia Pacific Seoul 1 Year Reserved m5 series
Asia Pacific Seoul 1 Year Reserved m5a series
Asia Pacific Seoul 1 Year Reserved m5ad series
Asia Pacific Seoul 1 Year Reserved m5d series
Asia Pacific Seoul 1 Year Reserved r5a series
Asia Pacific Seoul 1 Year Reserved r5ad series
Asia Pacific Seoul 1 Year Reserved z1d series
Asia Pacific Seoul 3 Year Reserved c5 series
Asia Pacific Seoul 3 Year Reserved c5d series
Asia Pacific Seoul 3 Year Reserved g4dn series
Asia Pacific Seoul 3 Year Reserved m4 series
Asia Pacific Seoul 3 Year Reserved m5 series
Asia Pacific Seoul 3 Year Reserved m5a series
Asia Pacific Seoul 3 Year Reserved m5ad series
Asia Pacific Seoul 3 Year Reserved m5d series
Asia Pacific Seoul 3 Year Reserved r5a series
Asia Pacific Seoul 3 Year Reserved r5ad series
Asia Pacific Seoul 3 Year Reserved z1d series
Asia Pacific Singapore 1 Year Reserved a1 series
Asia Pacific Singapore 1 Year Reserved c5d series
Asia Pacific Singapore 1 Year Reserved g4dn series
Asia Pacific Singapore 1 Year Reserved m4 series
Asia Pacific Singapore 1 Year Reserved m5 series
Asia Pacific Singapore 1 Year Reserved m5ad series
Asia Pacific Singapore 1 Year Reserved m5d series
Asia Pacific Singapore 1 Year Reserved m5dn series
Asia Pacific Singapore 1 Year Reserved m5n series
Asia Pacific Singapore 1 Year Reserved r5ad series
Asia Pacific Singapore 1 Year Reserved r5dn series
Asia Pacific Singapore 1 Year Reserved r5n series
Asia Pacific Singapore 3 Year Reserved a1 series
Asia Pacific Singapore 3 Year Reserved c5d series
Asia Pacific Singapore 3 Year Reserved g4dn series
Asia Pacific Singapore 3 Year Reserved m4 series
Asia Pacific Singapore 3 Year Reserved m5 series
Asia Pacific Singapore 3 Year Reserved m5ad series
Asia Pacific Singapore 3 Year Reserved m5d series
Asia Pacific Singapore 3 Year Reserved m5dn series
Asia Pacific Singapore 3 Year Reserved m5n series
Asia Pacific Singapore 3 Year Reserved r5ad series
Asia Pacific Singapore 3 Year Reserved r5dn series
Asia Pacific Singapore 3 Year Reserved r5n series
Asia Pacific Sydney 1 Year Reserved a1 series
Asia Pacific Sydney 1 Year Reserved c5d series
Asia Pacific Sydney 1 Year Reserved g4dn series
Asia Pacific Sydney 1 Year Reserved i3en series
Asia Pacific Sydney 1 Year Reserved m4 series
Asia Pacific Sydney 1 Year Reserved m5 series
Asia Pacific Sydney 1 Year Reserved m5ad series
Asia Pacific Sydney 1 Year Reserved m5d series
Asia Pacific Sydney 1 Year Reserved m5dn series
Asia Pacific Sydney 1 Year Reserved m5n series
Asia Pacific Sydney 1 Year Reserved r5ad series
Asia Pacific Sydney 1 Year Reserved r5dn series
Asia Pacific Sydney 1 Year Reserved r5n series
Asia Pacific Sydney 3 Year Reserved a1 series
Asia Pacific Sydney 3 Year Reserved c5d series
Asia Pacific Sydney 3 Year Reserved g4dn series
Asia Pacific Sydney 3 Year Reserved i3en series
Asia Pacific Sydney 3 Year Reserved m4 series
Asia Pacific Sydney 3 Year Reserved m5 series
Asia Pacific Sydney 3 Year Reserved m5ad series
Asia Pacific Sydney 3 Year Reserved m5d series
Asia Pacific Sydney 3 Year Reserved m5dn series
Asia Pacific Sydney 3 Year Reserved m5n series
Asia Pacific Sydney 3 Year Reserved r5ad series
Asia Pacific Sydney 3 Year Reserved r5dn series
Asia Pacific Sydney 3 Year Reserved r5n series
Asia Pacific Tokyo 1 Year Reserved a1 series
Asia Pacific Tokyo 1 Year Reserved c5d series
Asia Pacific Tokyo 1 Year Reserved g4dn series
Asia Pacific Tokyo 1 Year Reserved i3en series
Asia Pacific Tokyo 1 Year Reserved m4 series
Asia Pacific Tokyo 1 Year Reserved m5 series
Asia Pacific Tokyo 1 Year Reserved m5ad series
Asia Pacific Tokyo 1 Year Reserved m5d series
Asia Pacific Tokyo 1 Year Reserved m5dn series
Asia Pacific Tokyo 1 Year Reserved m5n series
Asia Pacific Tokyo 1 Year Reserved r5ad series
Asia Pacific Tokyo 1 Year Reserved r5dn series
Asia Pacific Tokyo 1 Year Reserved r5n series
Asia Pacific Tokyo 3 Year Reserved a1 series
Asia Pacific Tokyo 3 Year Reserved c5d series
Asia Pacific Tokyo 3 Year Reserved g4dn series
Asia Pacific Tokyo 3 Year Reserved i3en series
Asia Pacific Tokyo 3 Year Reserved m4 series
Asia Pacific Tokyo 3 Year Reserved m5 series
Asia Pacific Tokyo 3 Year Reserved m5ad series
Asia Pacific Tokyo 3 Year Reserved m5d series
Asia Pacific Tokyo 3 Year Reserved m5dn series
Asia Pacific Tokyo 3 Year Reserved m5n series
Asia Pacific Tokyo 3 Year Reserved r5ad series
Asia Pacific Tokyo 3 Year Reserved r5dn series
Asia Pacific Tokyo 3 Year Reserved r5n series
<table>
<thead>
<tr>
<th>Region</th>
<th>Service Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific Tokyo</td>
<td>3 Year Reserved c5d series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved g4dn series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved i3 series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m4 series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m5 series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m5ad series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m5d series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m5dn series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved m5n series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved r5ad series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved r5dn series</td>
</tr>
<tr>
<td></td>
<td>3 Year Reserved r5n series</td>
</tr>
<tr>
<td>Asia Seoul</td>
<td>c5 series</td>
</tr>
<tr>
<td></td>
<td>c5d series</td>
</tr>
<tr>
<td></td>
<td>g4dn series</td>
</tr>
<tr>
<td></td>
<td>m4 series</td>
</tr>
<tr>
<td></td>
<td>m5 series</td>
</tr>
<tr>
<td></td>
<td>m5a series</td>
</tr>
<tr>
<td></td>
<td>m5ad series</td>
</tr>
<tr>
<td></td>
<td>m5d series</td>
</tr>
<tr>
<td></td>
<td>m5dn series</td>
</tr>
<tr>
<td></td>
<td>m5n series</td>
</tr>
<tr>
<td></td>
<td>r5a series</td>
</tr>
<tr>
<td></td>
<td>r5ad series</td>
</tr>
<tr>
<td></td>
<td>r5dn series</td>
</tr>
<tr>
<td></td>
<td>r5n series</td>
</tr>
<tr>
<td>Asia Singapore</td>
<td>a1 series</td>
</tr>
<tr>
<td></td>
<td>c5d series</td>
</tr>
<tr>
<td></td>
<td>g4dn series</td>
</tr>
<tr>
<td></td>
<td>m4 series</td>
</tr>
<tr>
<td></td>
<td>m5 series</td>
</tr>
<tr>
<td></td>
<td>m5ad series</td>
</tr>
<tr>
<td></td>
<td>m5d series</td>
</tr>
<tr>
<td></td>
<td>m5dn series</td>
</tr>
<tr>
<td></td>
<td>m5n series</td>
</tr>
<tr>
<td></td>
<td>r5ad series</td>
</tr>
<tr>
<td></td>
<td>r5dn series</td>
</tr>
<tr>
<td></td>
<td>r5n series</td>
</tr>
<tr>
<td>Asia Tokyo</td>
<td>a1 series</td>
</tr>
<tr>
<td></td>
<td>c5d series</td>
</tr>
<tr>
<td></td>
<td>g4dn series</td>
</tr>
<tr>
<td></td>
<td>i3 series</td>
</tr>
<tr>
<td></td>
<td>m4 series</td>
</tr>
<tr>
<td></td>
<td>m5 series</td>
</tr>
<tr>
<td></td>
<td>m5ad series</td>
</tr>
<tr>
<td></td>
<td>m5d series</td>
</tr>
<tr>
<td></td>
<td>m5dn series</td>
</tr>
<tr>
<td></td>
<td>m5n series</td>
</tr>
<tr>
<td></td>
<td>r5ad series</td>
</tr>
<tr>
<td></td>
<td>r5dn series</td>
</tr>
<tr>
<td></td>
<td>r5n series</td>
</tr>
<tr>
<td>Canada Central</td>
<td>c5d series</td>
</tr>
<tr>
<td></td>
<td>c5n series</td>
</tr>
<tr>
<td></td>
<td>g4dn series</td>
</tr>
<tr>
<td></td>
<td>i3em series</td>
</tr>
<tr>
<td></td>
<td>m4 series</td>
</tr>
<tr>
<td></td>
<td>m5 series</td>
</tr>
<tr>
<td></td>
<td>m5ad series</td>
</tr>
<tr>
<td></td>
<td>m5d series</td>
</tr>
<tr>
<td></td>
<td>m5dn series</td>
</tr>
<tr>
<td></td>
<td>m5n series</td>
</tr>
</tbody>
</table>
Canada Central r5ad series
Canada Central x1e series
EU Frankfurt a1 series
EU Frankfurt c5d series
EU Frankfurt g4dn series
EU Frankfurt i3 series
EU Frankfurt m4 series
EU Frankfurt m5 series
EU Frankfurt m5ad series
EU Frankfurt m5d series
EU Frankfurt m5dn series
EU Frankfurt m5n series
EU Frankfurt r5ad series
EU Frankfurt r5dn series
EU Frankfurt r5n series
EU Frankfurt 1 Year Reserved a1 series
EU Frankfurt 1 Year Reserved c5d series
EU Frankfurt 1 Year Reserved g4dn series
EU Franklin 1 Year Reserved i3 series
EU Frankfurt 1 Year Reserved m4 series
EU Franklin 1 Year Reserved m5 series
EU Franklin 1 Year Reserved m5ad series
EU Franklin 1 Year Reserved m5d series
EU Franklin 1 Year Reserved m5dn series
EU Franklin 1 Year Reserved m5n series
EU Franklin 1 Year Reserved r5ad series
EU Franklin 1 Year Reserved r5dn series
EU Franklin 1 Year Reserved r5n series
EU Franklin 3 Year Reserved a1 series
EU Franklin 3 Year Reserved c5d series
EU Franklin 3 Year Reserved g4dn series
EU Franklin 3 Year Reserved i3 series
EU Franklin 3 Year Reserved m4 series
EU Franklin 3 Year Reserved m5 series
EU Franklin 3 Year Reserved m5ad series
EU Franklin 3 Year Reserved m5d series
EU Franklin 3 Year Reserved m5dn series
EU Franklin 3 Year Reserved m5n series
EU Franklin 3 Year Reserved r5ad series
EU Franklin 3 Year Reserved r5dn series
EU Franklin 3 Year Reserved r5n series
EU Ireland a1 series
EU Ireland c5d series
EU Ireland g4dn series
EU Ireland i3 series
EU Ireland m4 series
EU Ireland m5 series
EU Ireland m5ad series
EU Ireland m5d series
EU Ireland m5dn series
EU Ireland m5n series
EU Ireland r5ad series
EU Ireland r5dn series
EU Ireland r5n series
EU Ireland 1 Year Reserved a1 series
EU Ireland 1 Year Reserved c5d series
EU Ireland 1 Year Reserved g4dn series
EU Ireland 1 Year Reserved i3 series
EU Ireland 1 Year Reserved m4 series
EU Ireland 1 Year Reserved m5 series
EU Ireland 1 Year Reserved m5ad series
EU Ireland 1 Year Reserved m5d series
EU Ireland 1 Year Reserved m5dn series
EU Ireland 1 Year Reserved m5n series
EU Ireland 1 Year Reserved r5ad series
EU Ireland 1 Year Reserved r5dn series
EU Ireland 1 Year Reserved r5n series
EU Ireland 3 Year Reserved a1 series
EU Ireland 3 Year Reserved c5d series
EU Ireland 3 Year Reserved g4dn series
EU Ireland 3 Year Reserved i3 series
EU Ireland 3 Year Reserved m4 series
EU Ireland 3 Year Reserved m5 series
EU Ireland 3 Year Reserved m5ad series
EU Ireland 3 Year Reserved m5d series
EU Ireland 3 Year Reserved m5dn series
EU Ireland 3 Year Reserved m5n series
EU Ireland 3 Year Reserved r5ad series
EU Ireland 3 Year Reserved r5dn series
EU Ireland 3 Year Reserved r5n series
EU London 1 Year Reserved c5d series
EU London 1 Year Reserved g4dn series
EU London 1 Year Reserved i3en series
EU London 1 Year Reserved m4 series
EU London 1 Year Reserved m5 series
EU London 1 Year Reserved m5a series
EU London 1 Year Reserved m5ad series
EU London 1 Year Reserved m5d series
EU London 1 Year Reserved r5a series
EU London 1 Year Reserved r5ad series
EU London 1 Year Reserved r5dn series
EU London 1 Year Reserved r5n series
EU London 3 Year Reserved c5d series
EU London 3 Year Reserved g4dn series
EU London 3 Year Reserved i3en series
EU London 3 Year Reserved m4 series
EU London 3 Year Reserved m5a series
EU London 3 Year Reserved m5ad series
EU London 3 Year Reserved m5d series
EU London 3 Year Reserved r5a series
EU London 3 Year Reserved r5ad series
EU London 3 Year Reserved r5dn series
EU Paris g4dn series
EU Paris i3en series
EU Paris m5 series
EU Paris m5ad series
EU Paris m5d series
EU Paris r5ad series
EU Paris 1 Year Reserved g4dn series
EU Paris 1 Year Reserved i3en series
EU Paris 1 Year Reserved m5 series
EU Paris 1 Year Reserved m5ad series
EU Paris 1 Year Reserved m5d series
EU Paris 1 Year Reserved r5ad series
EU Paris 3 Year Reserved g4dn series
EU Paris 3 Year Reserved i3en series
EU Paris 3 Year Reserved m5 series
EU Paris 3 Year Reserved m5ad series
EU Paris 3 Year Reserved m5d series
EU Paris 3 Year Reserved r5ad series
EU Stockholm c5d series
EU Stockholm g4dn series
EU Stockholm m5 series
EU Stockholm m5d series
EU Stockholm 1 Year Reserved c5d series
EU Stockholm 1 Year Reserved g4dn series
EU Stockholm 1 Year Reserved m5 series
EU Stockholm 1 Year Reserved m5ad series
EU Stockholm 1 Year Reserved m5d series
EU Stockholm 3 Year Reserved c5d series
EU Stockholm 3 Year Reserved g4dn series
EU Stockholm 3 Year Reserved m5 series
EU Stockholm 3 Year Reserved m5ad series
EU Stockholm 3 Year Reserved m5d series
Middle East Bahrain 1 Year Reserved c5 series
Middle East Bahrain 1 Year Reserved c5d series
Middle East Bahrain 1 Year Reserved d2 series
Middle East Bahrain 1 Year Reserved g4dn series
Middle East Bahrain 1 Year Reserved i3 series
Middle East Bahrain 1 Year Reserved m5 series
Middle East Bahrain 1 Year Reserved m5ad series
Middle East Bahrain 1 Year Reserved m5d series
Middle East Bahrain 1 Year Reserved r5 series
Middle East Bahrain 1 Year Reserved r5ad series
Middle East Bahrain 3 Year Reserved c5 series
Middle East Bahrain 3 Year Reserved c5d series
Middle East Bahrain 3 Year Reserved d2 series
Middle East Bahrain 3 Year Reserved g4dn series
Middle East Bahrain 3 Year Reserved i3 series
Middle East Bahrain 3 Year Reserved m5 series
Middle East Bahrain 3 Year Reserved m5ad series
Middle East Bahrain 3 Year Reserved m5d series
Middle East Bahrain 3 Year Reserved r5 series
Middle East Bahrain 3 Year Reserved r5ad series
Pacific Sydney a1 series
Pacific Sydney c5d series
Pacific Sydney g4dn series
Pacific Sydney i3en series
Pacific Sydney m4 series
Pacific Sydney m5 series
Pacific Sydney m5ad series
Pacific Sydney m5d series
Pacific Sydney r5ad series
South America c5 series
South America c5d series
South America g4dn series
South America i3en series
South America m4 series
South America m5 series
South America m5a series
South America m5ad series
South America m5d series
South America r5 series
South America r5a series
South America r5ad series
South America r5d series
South America x1e series
South America Sao Paulo 1 Year Reserved c5 series
South America Sao Paulo 1 Year Reserved c5d series
South America Sao Paulo 1 Year Reserved g4dn series
South America Sao Paulo 1 Year Reserved i3en series
South America Sao Paulo 1 Year Reserved m4 series
South America Sao Paulo 1 Year Reserved m5 series
South America Sao Paulo 1 Year Reserved m5a series
South America Sao Paulo 1 Year Reserved m5ad series
South America Sao Paulo 1 Year Reserved m5d series
South America Sao Paulo 1 Year Reserved r5 series
South America Sao Paulo 1 Year Reserved r5a series
South America Sao Paulo 1 Year Reserved r5ad series
South America Sao Paulo 1 Year Reserved r5d series
South America Sao Paulo 1 Year Reserved x1e series
South America Sao Paulo 3 Year Reserved c5 series
South America Sao Paulo 3 Year Reserved c5d series
South America Sao Paulo 3 Year Reserved g4dn series
South America Sao Paulo 3 Year Reserved i3en series
South America Sao Paulo 3 Year Reserved m4 series
South America Sao Paulo 3 Year Reserved m5 series
South America Sao Paulo 3 Year Reserved m5a series
South America Sao Paulo 3 Year Reserved m5ad series
South America Sao Paulo 3 Year Reserved m5d series
South America Sao Paulo 3 Year Reserved r5 series
South America Sao Paulo 3 Year Reserved r5a series
South America Sao Paulo 3 Year Reserved r5ad series
South America Sao Paulo 3 Year Reserved r5d series
South America Sao Paulo 3 Year Reserved x1e series
US California c5d series
US California c5n series
US California g4dn series
US California i3 series
US California m4 series
US California m5 series
US California m5ad series
US California m5d series
US California r5ad series
US East 1 Year Reserved a1 series
US East 1 Year Reserved c5 series
US East 1 Year Reserved c5d series
US East 1 Year Reserved c5n series
US East 1 Year Reserved g4dn series
US East 1 Year Reserved i3 series
US East 1 Year Reserved i3en series
US East 1 Year Reserved m4 series
US East 1 Year Reserved m5 series
US East 1 Year Reserved m5a series
US East 1 Year Reserved m5d series
US East 1 Year Reserved m5dn series
US East 1 Year Reserved m5n series
US East 1 Year Reserved r5 series
US East 1 Year Reserved r5a series
US East 1 Year Reserved r5d series
US East 1 Year Reserved r5dn series
US East 1 Year Reserved r5n series
US East 3 Year Reserved a1 series
US East 3 Year Reserved c5 series
US East 3 Year Reserved c5d series
US East 3 Year Reserved c5n series
US East 3 Year Reserved g4dn series
US East 3 Year Reserved i3 series
US East 3 Year Reserved i3en series
US East 3 Year Reserved m4 series
US East 3 Year Reserved m5 series
US East 3 Year Reserved m5a series
US East 3 Year Reserved m5d series
US East 3 Year Reserved m5dn series
US East 3 Year Reserved m5n series
US East 3 Year Reserved r5 series
US East 3 Year Reserved r5a series
US East 3 Year Reserved r5d series
US East 3 Year Reserved r5dn series
US East 3 Year Reserved r5n series
US East Ohio 1 Year Reserved a1 series
US East Ohio 1 Year Reserved c5d series
US East Ohio 1 Year Reserved g4dn series
US East Ohio 1 Year Reserved i3 series
US East Ohio 1 Year Reserved m4 series
US East Ohio 1 Year Reserved m5 series
US East Ohio 1 Year Reserved m5a series
US East Ohio 1 Year Reserved m5d series
US East Ohio 1 Year Reserved m5dn series
US East Ohio 1 Year Reserved m5n series
US East Ohio 1 Year Reserved r5dn series
US East Ohio 1 Year Reserved r5n series
US East Ohio 3 Year Reserved z1d series
US East Ohio 3 Year Reserved a1 series
US East Ohio 3 Year Reserved c5d series
US East Ohio 3 Year Reserved g4dn series
US East Ohio 3 Year Reserved i3 series
US East Ohio 3 Year Reserved m4 series
US East Ohio 3 Year Reserved m5 series
US East Ohio 3 Year Reserved m5d series
US East Ohio 3 Year Reserved m5dn series
US East Ohio 3 Year Reserved m5n series
US East Ohio 3 Year Reserved r5dn series
US East Ohio 3 Year Reserved r5n series
US East Ohio 3 Year Reserved z1d series
US Ohio a1 series
US Ohio c5d series
US Ohio g4dn series
US Ohio i3 series
US Ohio m4 series
US Ohio m5 series
US Ohio m5d series
US Ohio m5dn series
US Ohio m5n series
US Ohio r5dn series
US Ohio r5n series
US Ohio z1d series
US Oregon a1 series
US Oregon c5d series
US Oregon g4dn series
US Oregon i3 series
US Oregon m4 series
US Oregon m5 series
US Oregon m5ad series
US Oregon m5d series
US Oregon m5dn series
US Oregon m5n series
US Oregon r5ad series
US Oregon r5dn series
US Oregon r5n series
US Virginia a1 series
US Virginia c5d series
US Virginia g4dn series
US Virginia i3 series
US Virginia m4 series
US Virginia m5 series
US Virginia m5ad series
US Virginia m5d series
US Virginia m5dn series
US Virginia m5n series
US Virginia m6g series
US Virginia r5dn series
US Virginia r5n series
US West Oregon 1 Year Reserved a1 series
US West Oregon 1 Year Reserved c5d series
US West Oregon 1 Year Reserved g4dn series
US West Oregon 1 Year Reserved i3 series
US West Oregon 1 Year Reserved m4 series
US West Oregon 1 Year Reserved m5 series
US West Oregon 1 Year Reserved m5ad series
US West Oregon 1 Year Reserved m5d series
US West Oregon 1 Year Reserved m5dn series
US West Oregon 1 Year Reserved m5n series
US West Oregon 1 Year Reserved r5ad series
US West Oregon 1 Year Reserved r5dn series
US West Oregon 1 Year Reserved r5n series
US West Oregon 3 Year Reserved a1 series
US West Oregon 3 Year Reserved c5d series
US West Oregon 3 Year Reserved g4dn series
US West Oregon 3 Year Reserved i3 series
US West Oregon 3 Year Reserved m4 series
US West Oregon 3 Year Reserved m5 series
US West Oregon 3 Year Reserved m5ad series
US West Oregon 3 Year Reserved m5d series
US West Oregon 3 Year Reserved m5dn series
US West Oregon 3 Year Reserved m5n series
US West Oregon 3 Year Reserved r5ad series
US West Oregon 3 Year Reserved r5dn series
US West Oregon 3 Year Reserved r5n series

Updated Instances
Asia Pacific Mumbai 1 Year Reserved c4 series
Asia Pacific Mumbai 1 Year Reserved c5 series
Asia Pacific Mumbai 1 Year Reserved c5d series
Asia Pacific Mumbai 1 Year Reserved c5n series
Asia Pacific Mumbai 1 Year Reserved d2 series
Asia Pacific Mumbai 1 Year Reserved i3 series
Asia Pacific Mumbai 1 Year Reserved m4 series
Asia Pacific Mumbai 1 Year Reserved r4 series
Asia Pacific Mumbai 1 Year Reserved r5 series
Asia Pacific Mumbai 1 Year Reserved r5d series
Asia Pacific Mumbai 1 Year Reserved r5n series
Asia Pacific Mumbai 1 Year Reserved x1 series
Asia Pacific Mumbai 3 Year Reserved c4 series
Asia Pacific Mumbai 3 Year Reserved c5 series
Asia Pacific Mumbai 3 Year Reserved c5d series
Asia Pacific Mumbai 3 Year Reserved c5n series
Asia Pacific Mumbai 3 Year Reserved d2 series
Asia Pacific Mumbai 3 Year Reserved i3 series
Asia Pacific Mumbai 3 Year Reserved m4 series
Asia Pacific Mumbai 3 Year Reserved r4 series
Asia Pacific Mumbai 3 Year Reserved r5 series
Asia Pacific Mumbai 3 Year Reserved r5d series
Asia Pacific Mumbai 3 Year Reserved r5n series
Asia Pacific Mumbai 3 Year Reserved x1 series
Asia Pacific Seoul 1 Year Reserved c4 series
Asia Pacific Seoul 1 Year Reserved c5 series
Asia Pacific Seoul 1 Year Reserved c5d series
Asia Pacific Seoul 1 Year Reserved c5n series
Asia Pacific Seoul 1 Year Reserved d2 series
Asia Pacific Seoul 1 Year Reserved i3 series
Asia Pacific Seoul 1 Year Reserved i3en series
Asia Pacific Seoul 1 Year Reserved m4 series
Asia Pacific Seoul 1 Year Reserved r4 series
Asia Pacific Seoul 1 Year Reserved r5 series
Asia Pacific Seoul 1 Year Reserved r5d series
Asia Pacific Seoul 1 Year Reserved x1 series
Asia Pacific Seoul 3 Year Reserved c4 series
Asia Pacific Seoul 3 Year Reserved c5 series
Asia Pacific Seoul 3 Year Reserved c5d series
Asia Pacific Seoul 3 Year Reserved c5n series
Asia Pacific Seoul 3 Year Reserved d2 series
Asia Pacific Seoul 3 Year Reserved i3 series
Asia Pacific Seoul 3 Year Reserved i3en series
Asia Pacific Seoul 3 Year Reserved m4 series
Asia Pacific Seoul 3 Year Reserved r4 series
Asia Pacific Seoul 3 Year Reserved r5 series
Asia Pacific Seoul 3 Year Reserved r5d series
Asia Pacific Seoul 3 Year Reserved x1 series
Asia Pacific Seoul 3 Year Reserved x1e series
Asia Pacific Singapore 1 Year Reserved c4 series
Asia Pacific Singapore 1 Year Reserved c5 series
Asia Pacific Singapore 1 Year Reserved c5d series
Asia Pacific Singapore 1 Year Reserved c5n series
Asia Pacific Singapore 1 Year Reserved d2 series
Asia Pacific Singapore 1 Year Reserved i3 series
Asia Pacific Singapore 1 Year Reserved i3en series
Asia Pacific Singapore 1 Year Reserved m4 series
Asia Pacific Singapore 1 Year Reserved m5a series
Asia Pacific Singapore 1 Year Reserved m5ad series
Asia Pacific Singapore 1 Year Reserved r4 series
Asia Pacific Singapore 1 Year Reserved r5 series
Asia Pacific Singapore 1 Year Reserved r5a series
Asia Pacific Singapore 1 Year Reserved r5ad series
Asia Pacific Singapore 1 Year Reserved r5d series
Asia Pacific Singapore 1 Year Reserved x1 series
Asia Pacific Singapore 1 Year Reserved x1e series
Asia Pacific Singapore 1 Year Reserved z1d series
Asia Pacific Singapore 3 Year Reserved c4 series
Asia Pacific Singapore 3 Year Reserved c5 series
Asia Pacific Singapore 3 Year Reserved c5d series
Asia Pacific Singapore 3 Year Reserved c5n series
Asia Pacific Singapore 3 Year Reserved d2 series
Asia Pacific Singapore 3 Year Reserved i3 series
Asia Pacific Singapore 3 Year Reserved i3en series
Asia Pacific Singapore 3 Year Reserved m4 series
Asia Pacific Singapore 3 Year Reserved m5a series
Asia Pacific Singapore 3 Year Reserved m5ad series
Asia Pacific Singapore 3 Year Reserved r4 series
Asia Pacific Singapore 3 Year Reserved r5 series
Asia Pacific Singapore 3 Year Reserved r5a series
Asia Pacific Singapore 3 Year Reserved r5ad series
Asia Pacific Singapore 3 Year Reserved r5d series
Asia Pacific Singapore 3 Year Reserved x1 series
Asia Pacific Singapore 3 Year Reserved x1e series
Asia Pacific Singapore 3 Year Reserved z1d series
Asia Pacific Sydney 1 Year Reserved c4 series
Asia Pacific Sydney 1 Year Reserved c5 series
Asia Pacific Sydney 1 Year Reserved c5d series
Asia Pacific Sydney 1 Year Reserved c5n series
Asia Pacific Sydney 1 Year Reserved d2 series
Asia Pacific Sydney 1 Year Reserved i3 series
Asia Pacific Sydney 1 Year Reserved m4 series
Asia Pacific Sydney 1 Year Reserved m5a series
Asia Pacific Sydney 1 Year Reserved m5ad series
Asia Pacific Sydney 1 Year Reserved r4 series
Asia Pacific Sydney 1 Year Reserved r5 series
Asia Pacific Sydney 1 Year Reserved r5a series
Asia Pacific Sydney 1 Year Reserved r5ad series
Asia Pacific Sydney 1 Year Reserved r5d series
Asia Pacific Sydney 1 Year Reserved x1 series
Asia Pacific Sydney 1 Year Reserved x1e series
Asia Pacific Sydney 1 Year Reserved z1d series
Asia Pacific Sydney 3 Year Reserved c4 series
Asia Pacific Sydney 3 Year Reserved c5 series
Asia Pacific Sydney 3 Year Reserved c5d series
Asia Pacific Sydney 3 Year Reserved c5n series
Asia Pacific Sydney 3 Year Reserved d2 series
Asia Pacific Sydney 3 Year Reserved i3 series
Asia Pacific Sydney 3 Year Reserved m4 series
Asia Pacific Sydney 3 Year Reserved m5a series
Asia Pacific Sydney 3 Year Reserved m5ad series
Asia Pacific Sydney 3 Year Reserved r4 series
Asia Pacific Sydney 3 Year Reserved r5 series
Asia Pacific Sydney 3 Year Reserved r5a series
Asia Pacific Sydney 3 Year Reserved r5ad series
Asia Pacific Sydney 3 Year Reserved r5d series
Asia Pacific Sydney 3 Year Reserved x1 series
Asia Pacific Sydney 3 Year Reserved x1e series
Asia Pacific Sydney 3 Year Reserved z1d series
Asia Pacific Tokyo 1 Year Reserved c4 series
Asia Pacific Tokyo 1 Year Reserved c5 series
Asia Pacific Tokyo 1 Year Reserved c5d series
Asia Pacific Tokyo 1 Year Reserved c5n series
Asia Pacific Tokyo 1 Year Reserved d2 series
Asia Pacific Tokyo 1 Year Reserved i3 series
Asia Pacific Tokyo 1 Year Reserved i3en series
Asia Pacific Tokyo 1 Year Reserved m4 series
Asia Pacific Tokyo 1 Year Reserved m5a series
Asia Pacific Tokyo 1 Year Reserved r4 series
Asia Pacific Tokyo 1 Year Reserved r5 series
Asia Pacific Tokyo 1 Year Reserved r5a series
Asia Pacific Tokyo 1 Year Reserved r5d series
Asia Pacific Tokyo 1 Year Reserved x1 series
Asia Pacific Tokyo 1 Year Reserved x1e series
Asia Pacific Tokyo 1 Year Reserved z1d series
Asia Pacific Tokyo 1 Year Reserved m5a series
Asia Pacific Tokyo 1 Year Reserved m5ad series
Asia Pacific Tokyo 1 Year Reserved r5ad series
Asia Pacific Tokyo 1 Year Reserved r5d series
Asia Pacific Tokyo 1 Year Reserved x1 series
Asia Pacific Tokyo 1 Year Reserved x1e series
Asia Pacific Tokyo 1 Year Reserved z1d series
Asia Pacific Tokyo 1 Year Reserved c4 series
Asia Pacific Tokyo 1 Year Reserved c5 series
Asia Pacific Tokyo 1 Year Reserved c5d series
Asia Pacific Tokyo 1 Year Reserved c5n series
Asia Pacific Tokyo 3 Year Reserved d2 series
Asia Pacific Tokyo 3 Year Reserved i3 series
Asia Pacific Tokyo 3 Year Reserved i3en series
Asia Pacific Tokyo 3 Year Reserved m4 series
Asia Pacific Tokyo 3 Year Reserved m5a series
Asia Pacific Tokyo 3 Year Reserved r4 series
Asia Pacific Tokyo 3 Year Reserved r5 series
Asia Pacific Tokyo 3 Year Reserved r5a series
Asia Pacific Tokyo 3 Year Reserved r5d series
Asia Pacific Tokyo 3 Year Reserved x1 series
Asia Pacific Tokyo 3 Year Reserved x1e series
Asia Pacific Tokyo 3 Year Reserved z1d series
EU Frankfurt 1 Year Reserved c4 series
EU Frankfurt 1 Year Reserved c5 series
EU Frankfurt 1 Year Reserved c5d series
EU Frankfurt 1 Year Reserved c5n series
EU Frankfurt 1 Year Reserved d2 series
EU Frankfurt 1 Year Reserved i3 series
EU Frankfurt 1 Year Reserved i3en series
EU Frankfurt 1 Year Reserved m4 series
EU Frankfurt 1 Year Reserved m5a series
EU Frankfurt 1 Year Reserved r4 series
EU Frankfurt 1 Year Reserved r5 series
EU Frankfurt 1 Year Reserved m5ad series
EU Frankfurt 1 Year Reserved r5ad series
EU Frankfurt 1 Year Reserved r5d series
EU Frankfurt 1 Year Reserved x1 series
EU Frankfurt 1 Year Reserved x1e series
EU Frankfurt 1 Year Reserved z1d series
EU Frankfurt 1 Year Reserved r5a series
EU Frankfurt 1 Year Reserved r5d series
EU Frankfurt 1 Year Reserved x1 series
EU Frankfurt 1 Year Reserved x1e series
EU Frankfurt 1 Year Reserved z1d series
EU Frankfurt 3 Year Reserved c4 series
EU Frankfurt 3 Year Reserved c5 series
EU Frankfurt 3 Year Reserved c5d series
EU Frankfurt 3 Year Reserved c5n series
EU Frankfurt 3 Year Reserved d2 series
EU Frankfurt 3 Year Reserved i3 series
EU Frankfurt 3 Year Reserved i3en series
EU Frankfurt 3 Year Reserved m4 series
EU Frankfurt 3 Year Reserved m5a series
EU Frankfurt 3 Year Reserved r4 series
EU Frankfurt 3 Year Reserved r5 series
EU Frankfurt 3 Year Reserved r5a series
EU Frankfurt 3 Year Reserved r5d series
EU Frankfurt 3 Year Reserved x1 series
EU Frankfurt 3 Year Reserved x1e series
EU Frankfurt 3 Year Reserved z1d series
EU Ireland 1 Year Reserved c4 series
EU Ireland 1 Year Reserved c5 series
EU Ireland 1 Year Reserved c5d series
EU Ireland 1 Year Reserved c5n series
EU Ireland 1 Year Reserved d2 series
EU Ireland 1 Year Reserved h1 series
EU Ireland 1 Year Reserved i3 series
EU Ireland 1 Year Reserved i3en series
EU Ireland 1 Year Reserved m4 series
EU Ireland 1 Year Reserved m5a series
EU Ireland 1 Year Reserved r4 series
EU Ireland 1 Year Reserved r5 series
EU Ireland 1 Year Reserved r5a series
EU Ireland 1 Year Reserved r5d series
EU Ireland 1 Year Reserved x1 series
EU Ireland 1 Year Reserved x1e series
EU Ireland 3 Year Reserved c4 series
EU Ireland 3 Year Reserved c5 series
EU Ireland 3 Year Reserved c5d series
EU Ireland 3 Year Reserved c5n series
EU Ireland 3 Year Reserved d2 series
EU Ireland 3 Year Reserved h1 series
EU Ireland 3 Year Reserved i3 series
EU Ireland 3 Year Reserved i3en series
EU Ireland 3 Year Reserved m4 series
EU Ireland 3 Year Reserved m5a series
EU Ireland 3 Year Reserved r4 series
EU Ireland 3 Year Reserved r5 series
EU Ireland 3 Year Reserved r5a series
EU Ireland 3 Year Reserved r5d series
EU Ireland 3 Year Reserved x1 series
EU Ireland 3 Year Reserved x1e series
EU Ireland 3 Year Reserved z1d series
EU London 1 Year Reserved c4 series
Chapter 4  Using the Platform
Reports/Pages

EU London 1 Year Reserved c5 series
EU London 1 Year Reserved c5d series
EU London 1 Year Reserved d2 series
EU London 1 Year Reserved i3 series
EU London 1 Year Reserved m4 series
EU London 1 Year Reserved r4 series
EU London 1 Year Reserved r5 series
EU London 1 Year Reserved r5d series
EU London 1 Year Reserved x1 series
EU London 1 Year Reserved z1d series
EU London 3 Year Reserved c4 series
EU London 3 Year Reserved c5 series
EU London 3 Year Reserved c5d series
EU London 3 Year Reserved d2 series
EU London 3 Year Reserved i3 series
EU London 3 Year Reserved m4 series
EU London 3 Year Reserved r4 series
EU London 3 Year Reserved r5 series
EU London 3 Year Reserved r5d series
EU London 3 Year Reserved x1 series
EU London 3 Year Reserved z1d series
EU Paris 1 Year Reserved c5 series
EU Paris 1 Year Reserved c5d series
EU Paris 1 Year Reserved d2 series
EU Paris 1 Year Reserved i3 series
EU Paris 1 Year Reserved m5a series
EU Paris 1 Year Reserved r4 series
EU Paris 1 Year Reserved r5 series
EU Paris 1 Year Reserved r5a series
EU Paris 1 Year Reserved x1 series
EU Paris 3 Year Reserved c5 series
EU Paris 3 Year Reserved c5d series
EU Paris 3 Year Reserved d2 series
EU Paris 3 Year Reserved i3 series
EU Paris 3 Year Reserved m5a series
EU Paris 3 Year Reserved r4 series
EU Paris 3 Year Reserved r5 series
EU Paris 3 Year Reserved r5a series
EU Paris 3 Year Reserved r5d series
EU Paris 3 Year Reserved x1 series
EU Stockholm 1 Year Reserved c5 series
EU Stockholm 1 Year Reserved c5d series
EU Stockholm 1 Year Reserved d2 series
EU Stockholm 1 Year Reserved i3 series
EU Stockholm 1 Year Reserved r5 series
EU Stockholm 1 Year Reserved r5d series
EU Stockholm 3 Year Reserved c5 series
EU Stockholm 3 Year Reserved c5d series
EU Stockholm 3 Year Reserved d2 series
EU Stockholm 3 Year Reserved i3 series
EU Stockholm 3 Year Reserved r5 series
EU Stockholm 3 Year Reserved r5d series
EU Stockholm 3 Year Reserved r5a series
EU Stockholm 3 Year Reserved x1 series
South America i3 series
South America Sao Paulo 1 Year Reserved c4 series
South America Sao Paulo 1 Year Reserved c5 series
South America Sao Paulo 1 Year Reserved i3 series
South America Sao Paulo 1 Year Reserved m4 series
South America Sao Paulo 1 Year Reserved r4 series
South America Sao Paulo 1 Year Reserved x1 series
South America Sao Paulo 3 Year Reserved c4 series
South America Sao Paulo 3 Year Reserved c5 series
South America Sao Paulo 3 Year Reserved i3 series
South America Sao Paulo 3 Year Reserved m4 series
South America Sao Paulo 3 Year Reserved r4 series
South America Sao Paulo 3 Year Reserved x1 series
US East 1 Year Reserved c4 series
US East 1 Year Reserved c5 series
US East 1 Year Reserved c5d series
US East 1 Year Reserved c5n series
US East 1 Year Reserved d2 series
US East 1 Year Reserved h1 series
US East 1 Year Reserved i3 series
US East 1 Year Reserved m4 series
US East 1 Year Reserved m5a series
US East 1 Year Reserved m5ad series
US East 1 Year Reserved r4 series
US East 1 Year Reserved r5 series
US East 1 Year Reserved r5a series
US East 1 Year Reserved r5ad series
US East 1 Year Reserved x1 series
US East 1 Year Reserved x1e series
US East 1 Year Reserved z1d series
US East 3 Year Reserved c4 series
US East 3 Year Reserved c5 series
US East 3 Year Reserved c5d series
US East 3 Year Reserved c5n series
US East 3 Year Reserved d2 series
US East 3 Year Reserved h1 series
US East 3 Year Reserved i3 series
US East 3 Year Reserved m4 series
US East 3 Year Reserved m5a series
US East 3 Year Reserved m5ad series
US East 3 Year Reserved r4 series
US East 3 Year Reserved r5 series
US East 3 Year Reserved r5a series
US East 3 Year Reserved r5ad series
US East 3 Year Reserved r5d series
US East 3 Year Reserved x1 series
US East 3 Year Reserved x1e series
US East 3 Year Reserved z1d series
US East Ohio 1 Year Reserved c4 series
US East Ohio 1 Year Reserved c5 series
US East Ohio 1 Year Reserved c5d series
US East Ohio 1 Year Reserved c5n series
US East Ohio 1 Year Reserved d2 series
US East Ohio 1 Year Reserved h1 series
US East Ohio 1 Year Reserved i3 series
US East Ohio 1 Year Reserved i3en series
US East Ohio 1 Year Reserved m4 series
US East Ohio 1 Year Reserved m5a series
US East Ohio 1 Year Reserved m5ad series
US East Ohio 1 Year Reserved r4 series
US East Ohio 1 Year Reserved r5 series
US East Ohio 1 Year Reserved r5a series
US East Ohio 1 Year Reserved r5ad series
US East Ohio 1 Year Reserved r5d series
US East Ohio 1 Year Reserved x1 series
US East Ohio 1 Year Reserved x1e series
US East Ohio 3 Year Reserved c4 series
US East Ohio 3 Year Reserved c5 series
US East Ohio 3 Year Reserved c5d series
US East Ohio 3 Year Reserved c5n series
US East Ohio 3 Year Reserved d2 series
US East Ohio 3 Year Reserved h1 series
US East Ohio 3 Year Reserved i3 series
US East Ohio 3 Year Reserved i3en series
US East Ohio 3 Year Reserved m4 series
US East Ohio 3 Year Reserved m5a series
US East Ohio 3 Year Reserved m5ad series
US East Ohio 3 Year Reserved r4 series
US East Ohio 3 Year Reserved r5 series
US East Ohio 3 Year Reserved r5a series
US East Ohio 3 Year Reserved r5ad series
US East Ohio 3 Year Reserved r5d series
US East Ohio 3 Year Reserved x1 series
US East Ohio 3 Year Reserved x1e series
US West Oregon 1 Year Reserved c4 series
US West Oregon 1 Year Reserved c5 series
US West Oregon 1 Year Reserved c5d series
US West Oregon 1 Year Reserved c5n series
US West Oregon 1 Year Reserved d2 series
US West Oregon 1 Year Reserved h1 series
US West Oregon 1 Year Reserved i3 series
US West Oregon 1 Year Reserved i3en series
US West Oregon 1 Year Reserved m4 series
US West Oregon 1 Year Reserved m5a series
US West Oregon 1 Year Reserved m5ad series
US West Oregon 1 Year Reserved r4 series
US West Oregon 1 Year Reserved r5 series
US West Oregon 1 Year Reserved r5a series
US West Oregon 1 Year Reserved r5ad series
US West Oregon 1 Year Reserved r5d series
US West Oregon 3 Year Reserved c4 series
US West Oregon 3 Year Reserved c5 series
US West Oregon 3 Year Reserved c5d series
US West Oregon 3 Year Reserved c5n series
US West Oregon 3 Year Reserved d2 series
US West Oregon 3 Year Reserved h1 series
US West Oregon 3 Year Reserved i3 series
US West Oregon 3 Year Reserved i3en series
US West Oregon 3 Year Reserved m4 series
US West Oregon 3 Year Reserved m5a series
US West Oregon 3 Year Reserved m5ad series
US West Oregon 3 Year Reserved r4 series
US West Oregon 3 Year Reserved r5 series
US West Oregon 3 Year Reserved r5a series
US West Oregon 3 Year Reserved r5ad series
US West Oregon 3 Year Reserved r5d series
US West Oregon 3 Year Reserved x1 series
US West Oregon 3 Year Reserved x1e series
US West Oregon 3 Year Reserved z1d series
US West Oregon 3 Year Reserved c4 series
US West Oregon 3 Year Reserved c5 series
US West Oregon 3 Year Reserved c5d series
US West Oregon 3 Year Reserved c5n series
US West Oregon 3 Year Reserved d2 series
US West Oregon 3 Year Reserved h1 series
US West Oregon 3 Year Reserved i3 series
US West Oregon 3 Year Reserved i3en series
US West Oregon 3 Year Reserved m4 series
US West Oregon 3 Year Reserved m5a series
US West Oregon 3 Year Reserved m5ad series
US West Oregon 3 Year Reserved r4 series
US West Oregon 3 Year Reserved r5 series
US West Oregon 3 Year Reserved r5a series
US West Oregon 3 Year Reserved r5ad series
US West Oregon 3 Year Reserved r5d series
US West Oregon 3 Year Reserved x1 series
US West Oregon 3 Year Reserved x1e series
US West Oregon 3 Year Reserved z1d series

**Azure Updates / April 1, 2020**

- New Locations
- New Instances

**New Locations**

East US 1 Year Reserved
East US 3 Year Reserved
Central US 1 Year Reserved
Central US 3 Year Reserved
East US 2 1 Year Reserved
East US 2 3 Year Reserved
North Central US 1 Year Reserved
North Central US 3 Year Reserved
South Central US 1 Year Reserved
South Central US 3 Year Reserved
West US 1 Year Reserved
West US 3 Year Reserved
US Gov Iowa 1 Year Reserved
US Gov Iowa 3 Year Reserved
US Gov Virginia 1 Year Reserved
US Gov Virginia 3 Year Reserved
North Europe 1 Year Reserved
North Europe 3 Year Reserved
West Europe 1 Year Reserved
West Europe 3 Year Reserved
Australia East 1 Year Reserved
Australia East 3 Year Reserved
Australia Southeast 1 Year Reserved
Australia Southeast 3 Year Reserved
West Central US 1 Year Reserved
West Central US 3 Year Reserved
West US 2 1 Year Reserved
West US 2 3 Year Reserved
East Asia 1 Year Reserved
East Asia 3 Year Reserved
Southeast Asia 1 Year Reserved
Southeast Asia 3 Year Reserved
Japan East 1 Year Reserved
Japan East 3 Year Reserved
Japan West 1 Year Reserved
Japan West 3 Year Reserved
Brazil South 1 Year Reserved
Brazil South 3 Year Reserved
Central India 1 Year Reserved
Central India 3 Year Reserved
South India 1 Year Reserved
South India 3 Year Reserved
Canada Central 1 Year Reserved
Canada Central 3 Year Reserved
Canada East 1 Year Reserved
Canada East 3 Year Reserved
Germany Central 1 Year Reserved
Germany Central 3 Year Reserved
Germany Northeast 1 Year Reserved
Germany Northeast 3 Year Reserved
UK South 1 Year Reserved
UK South 3 Year Reserved
UK West 1 Year Reserved
UK West 3 Year Reserved
West India 1 Year Reserved
West India 3 Year Reserved
Korea Central 1 Year Reserved
Korea Central 3 Year Reserved
Korea South 1 Year Reserved
Korea South 3 Year Reserved
US Gov Arizona 1 Year Reserved
US Gov Arizona 3 Year Reserved
US Gov Texas 1 Year Reserved
US Gov Texas 3 Year Reserved
Australia Central 1 Year Reserved
Australia Central 3 Year Reserved
France South 1 Year Reserved
France South 3 Year Reserved
Australia Central 2 1 Year Reserved
Australia Central 2 3 Year Reserved
France Central 1 Year Reserved
France Central 3 Year Reserved

**New Instances**

Australia Central a series
Australia Central am series
Australia Central d series
Australia Central ds series
Australia Central e series
Australia Central e-4s series
Australia Central e-8s series
Australia Central es series
Australia Central f series
Australia Central f1 series
Australia Central f4 series
Australia Central fs series
Australia Central m series
Australia Central m-16ms series
Australia Central m-32ms series
Australia Central m-64ms series
Australia Central m-8ms series
Australia Central mls series
Australia Central mm series
Australia Central mms series
Australia Central ms series
Australia Central mts series
Chapter 4 Using the Platform

Reports/Pages

Australia Central 1 Year Reserved a series
Australia Central 1 Year Reserved am series
Australia Central 1 Year Reserved d series
Australia Central 1 Year Reserved ds series
Australia Central 1 Year Reserved e series
Australia Central 1 Year Reserved e-2s series
Australia Central 1 Year Reserved e-32s series
Australia Central 1 Year Reserved e-4s series
Australia Central 1 Year Reserved e-8s series
Australia Central 1 Year Reserved es series
Australia Central 1 Year Reserved f series
Australia Central 1 Year Reserved f1 series
Australia Central 1 Year Reserved f4 series
Australia Central 1 Year Reserved fs series
Australia Central 1 Year Reserved m series
Australia Central 1 Year Reserved m-16ms series
Australia Central 1 Year Reserved m-32ms series
Australia Central 1 Year Reserved m-64ms series
Australia Central 1 Year Reserved m-8ms series
Australia Central 1 Year Reserved mls series
Australia Central 1 Year Reserved mm series
Australia Central 1 Year Reserved mms series
Australia Central 1 Year Reserved ms series
Australia Central 1 Year Reserved mts series
Australia Central 2 a series
Australia Central 2 am series
Australia Central 2 d series
Australia Central 2 ds series
Australia Central 2 e series
Australia Central 2 e-4s series
Australia Central 2 e-8s series
Australia Central 2 es series
Australia Central 2 f series
Australia Central 2 f1 series
Australia Central 2 f4 series
Australia Central 2 fs series
Australia Central 2 m series
Australia Central 2 m-16ms series
Australia Central 2 m-32ms series
Australia Central 2 m-64ms series
Australia Central 2 m-8ms series
Australia Central 2 mls series
Australia Central 2 mm series
Australia Central 2 mms series
Australia Central 2 ms series
Australia Central 2 mts series
Australia Central 2 1 Year Reserved a series
Australia Central 2 1 Year Reserved am series
Australia Central 2 1 Year Reserved d series
Australia Central 2 1 Year Reserved ds series
Australia Central 2 1 Year Reserved e series
Australia Central 2 1 Year Reserved e-2s series
Australia Central 2 1 Year Reserved e-32s series
Australia Central 2 1 Year Reserved e-4s series
Australia Central 2 1 Year Reserved e-8s series
Australia Central 2 1 Year Reserved es series
Australia Central 2 1 Year Reserved f series
Australia Central 2 1 Year Reserved f1 series
Australia Central 2 1 Year Reserved f4 series
Australia Central 2 1 Year Reserved fs series
Australia Central 2 1 Year Reserved m series
Australia Central 2 1 Year Reserved m-16ms series
Australia Central 2 1 Year Reserved m-32ms series
Australia Central 2 1 Year Reserved m-64ms series
Australia Central 2 1 Year Reserved m-8ms series
Australia Central 2 1 Year Reserved mls series
Australia Central 2 1 Year Reserved mm series
Australia Central 2 1 Year Reserved mms series
Australia Central 2 1 Year Reserved ms series
Australia Central 2 1 Year Reserved mts series
Australia Central 2 3 Year Reserved a series
Australia Central 2 3 Year Reserved am series
Australia Central 2 3 Year Reserved d series
Australia Central 2 3 Year Reserved ds series
Australia Central 2 3 Year Reserved e series
Australia Central 2 3 Year Reserved e-2s series
Australia Central 2 3 Year Reserved e-32s series
Australia Central 2 3 Year Reserved e-4s series
Australia Central 2 3 Year Reserved e-8s series
Australia Central 2 3 Year Reserved es series
Australia Central 2 3 Year Reserved f series
Australia Central 2 3 Year Reserved f1 series
Australia Central 2 3 Year Reserved f4 series
Australia Central 2 3 Year Reserved fs series
Australia Central 2 3 Year Reserved m series
Australia Central 2 3 Year Reserved m-16ms series
Australia Central 2 3 Year Reserved m-32ms series
Australia Central 2 3 Year Reserved m-64ms series
Australia Central 2 3 Year Reserved m-8ms series
Australia Central 2 3 Year Reserved mls series
Australia Central 2 3 Year Reserved mm series
Australia Central 2 3 Year Reserved mms series
Australia Central 2 3 Year Reserved ms series
Australia Central 2 3 Year Reserved mts series
Australia Central 3 Year Reserved a series
Australia Central 3 Year Reserved am series
Australia Central 3 Year Reserved d series
Australia Central 3 Year Reserved ds series
Australia Central 3 Year Reserved e series
Australia Central 3 Year Reserved e-2s series
Australia Central 3 Year Reserved e-32s series
Australia Central 3 Year Reserved e-4s series
Australia Central 3 Year Reserved e-8s series
Australia Central 3 Year Reserved es series
Australia Central 3 Year Reserved f series
Australia Central 3 Year Reserved f1 series
Australia Central 3 Year Reserved f4 series
Australia Central 3 Year Reserved fs series
Australia Central 3 Year Reserved m series
Australia Central 3 Year Reserved m-16ms series
Australia Central 3 Year Reserved m-32ms series
Australia Central 3 Year Reserved m-64ms series
Australia Central 3 Year Reserved m-8ms series
Australia Central 3 Year Reserved mls series
Australia Central 3 Year Reserved mm series
Australia Central 3 Year Reserved mms series
Australia Central 3 Year Reserved ms series
Australia Central 3 Year Reserved mts series
Australia East d series
Australia East ds series
Australia East ls series
Australia East m-8ms series
Australia East mms series
Australia East ms series
Australia East 1 Year Reserved a series
Australia East 1 Year Reserved am series
Australia East 1 Year Reserved d series
Australia East 1 Year Reserved ds series
Australia East 1 Year Reserved e series
Australia East 1 Year Reserved e-2s series
Australia East 1 Year Reserved e-32s series
Australia East 1 Year Reserved e-4s series
Australia East 1 Year Reserved e-8s series
Australia East 1 Year Reserved ei series
Australia East 1 Year Reserved eis series
Australia East 1 Year Reserved es series
Australia East 1 Year Reserved f series
Australia East 1 Year Reserved f1 series
Australia East 1 Year Reserved f4 series
Australia East 1 Year Reserved fs series
Australia East 1 Year Reserved g series
Australia East 1 Year Reserved gs series
Australia East 1 Year Reserved h series
Australia East 1 Year Reserved ls series
Australia East 1 Year Reserved m series
Australia East 1 Year Reserved m-16ms series
Australia East 1 Year Reserved m-32ms series
Australia East 1 Year Reserved m-64ms series
Australia East 1 Year Reserved m-8ms series
Australia East 1 Year Reserved mls series
Australia East 1 Year Reserved mm series
Australia East 1 Year Reserved mms series
Australia East 1 Year Reserved ms series
Australia East 1 Year Reserved mts series
Australia East 3 Year Reserved a series
Australia East 3 Year Reserved am series
Australia East 3 Year Reserved d series
Australia East 3 Year Reserved ds series
Australia East 3 Year Reserved e series
Australia East 3 Year Reserved e-2s series
Australia East 3 Year Reserved e-32s series
Australia East 3 Year Reserved e-4s series
Australia East 3 Year Reserved e-8s series
Australia East 3 Year Reserved ei series
Australia East 3 Year Reserved eis series
Australia East 3 Year Reserved es series
Australia East 3 Year Reserved f series
Australia East 3 Year Reserved f1 series
Australia East 3 Year Reserved f4 series
Australia East 3 Year Reserved fs series
Australia East 3 Year Reserved g series
Australia East 3 Year Reserved gs series
Australia East 3 Year Reserved h series
Australia East 3 Year Reserved ls series
Australia East 3 Year Reserved m series
Australia East 3 Year Reserved m-16ms series
Australia East 3 Year Reserved m-32ms series
Australia East 3 Year Reserved m-64ms series
Australia East 3 Year Reserved m-8ms series
Australia East 3 Year Reserved mls series
Australia East 3 Year Reserved mm series
Australia East 3 Year Reserved mms series
Australia East 3 Year Reserved ms series
Australia East 3 Year Reserved mts series
Australia Southeast d series
Australia Southeast ds series
Australia Southeast m-8ms series
Australia Southeast mms series
Australia Southeast ms series
Australia Southeast mts series
Australia Southeast 1 Year Reserved a series
Australia Southeast 1 Year Reserved am series
Australia Southeast 1 Year Reserved d series
Australia Southeast 1 Year Reserved ds series
Australia Southeast 1 Year Reserved e series
Australia Southeast 1 Year Reserved e-2s series
Australia Southeast 1 Year Reserved e-32s series
Australia Southeast 1 Year Reserved e-4s series
Australia Southeast 1 Year Reserved e-8s series
Australia Southeast 1 Year Reserved ei series
Australia Southeast 1 Year Reserved eis series
Australia Southeast 1 Year Reserved es series
Australia Southeast 1 Year Reserved f series
Australia Southeast 1 Year Reserved f1 series
Australia Southeast 1 Year Reserved f4 series
Australia Southeast 1 Year Reserved fs series
Australia Southeast 1 Year Reserved m series
Australia Southeast 1 Year Reserved m-16ms series
Australia Southeast 1 Year Reserved m-32ms series
Australia Southeast 1 Year Reserved m-64ms series
Australia Southeast 1 Year Reserved m-8ms series
Australia Southeast 1 Year Reserved mls series
Australia Southeast 1 Year Reserved mm series
Australia Southeast 1 Year Reserved mms series
Australia Southeast 1 Year Reserved ms series
Australia Southeast 1 Year Reserved mts series
Australia Southeast 3 Year Reserved a series
Australia Southeast 3 Year Reserved am series
Australia Southeast 3 Year Reserved d series
Australia Southeast 3 Year Reserved ds series
Australia Southeast 3 Year Reserved e series
Australia Southeast 3 Year Reserved e-2s series
Australia Southeast 3 Year Reserved e-32s series
Australia Southeast 3 Year Reserved e-4s series
Australia Southeast 3 Year Reserved e-8s series
Australia Southeast 3 Year Reserved e1 series
Australia Southeast 3 Year Reserved e1s series
Australia Southeast 3 Year Reserved es series
Australia Southeast 3 Year Reserved f series
Australia Southeast 3 Year Reserved f1 series
Australia Southeast 3 Year Reserved f4 series
Australia Southeast 3 Year Reserved fs series
Australia Southeast 3 Year Reserved m series
Australia Southeast 3 Year Reserved m-16ms series
Australia Southeast 3 Year Reserved m-32ms series
Australia Southeast 3 Year Reserved m-64ms series
Australia Southeast 3 Year Reserved m-8ms series
Australia Southeast 3 Year Reserved mls series
Australia Southeast 3 Year Reserved mm series
Australia Southeast 3 Year Reserved mms series
Australia Southeast 3 Year Reserved ms series
Australia Southeast 3 Year Reserved mts series
Brazil South d series
Brazil South ds series
Brazil South m-8ms series
Brazil South 1 Year Reserved a series
Brazil South 1 Year Reserved am series
Brazil South 1 Year Reserved d series
Brazil South 1 Year Reserved ds series
Brazil South 1 Year Reserved e series
Brazil South 1 Year Reserved e-2s series
Brazil South 1 Year Reserved e-32s series
Brazil South 1 Year Reserved e-4s series
Brazil South 1 Year Reserved e-8s series
Brazil South 1 Year Reserved ei series
Brazil South 1 Year Reserved eis series
Brazil South 1 Year Reserved es series
Brazil South 1 Year Reserved f series
Brazil South 1 Year Reserved f1 series
Brazil South 1 Year Reserved f4 series
Brazil South 1 Year Reserved fs series
Brazil South 1 Year Reserved m series
Brazil South 1 Year Reserved m-16ms series
Brazil South 1 Year Reserved m-32ms series
Brazil South 1 Year Reserved m-64ms series
Brazil South 1 Year Reserved m-8ms series
Brazil South 1 Year Reserved mls series
Brazil South 1 Year Reserved mm series
Brazil South 1 Year Reserved mms series
Brazil South 1 Year Reserved ms series
Brazil South 1 Year Reserved mts series
Brazil South 3 Year Reserved a series
Brazil South 3 Year Reserved am series
Brazil South 3 Year Reserved d series
Brazil South 3 Year Reserved ds series
Brazil South 3 Year Reserved e series
Brazil South 3 Year Reserved e-2s series
Brazil South 3 Year Reserved e-32s series
Brazil South 3 Year Reserved e-4s series
Brazil South 3 Year Reserved e-8s series
Brazil South 3 Year Reserved ei series
Brazil South 3 Year Reserved eis series
Brazil South 3 Year Reserved es series
Brazil South 3 Year Reserved f series
Brazil South 3 Year Reserved f1 series
Brazil South 3 Year Reserved f4 series
Brazil South 3 Year Reserved fs series
Brazil South 3 Year Reserved m series
Brazil South 3 Year Reserved m-16ms series
Brazil South 3 Year Reserved m-32ms series
Brazil South 3 Year Reserved m-64ms series
Brazil South 3 Year Reserved m-8ms series
Brazil South 3 Year Reserved mls series
Brazil South 3 Year Reserved mm series
Brazil South 3 Year Reserved mms series
Brazil South 3 Year Reserved ms series
Brazil South 3 Year Reserved mts series
Canada Central a series
Canada Central am series
Canada Central d series
Canada Central dc1s-v2 series
Canada Central dc2s-v2 series
Canada Central dc4s-v2 series
Canada Central dc8s-v2 series
Canada Central ds series
Canada Central f series
Canada Central fs series
Canada Central g series
Canada Central gs series
Canada Central ls series
Canada Central m-8ms series
Canada Central 1 Year Reserved a series
Canada Central 1 Year Reserved am series
Canada Central 1 Year Reserved d series
Canada Central 1 Year Reserved dc1s-v2 series
Canada Central 1 Year Reserved dc2s-v2 series
Canada Central 1 Year Reserved dc4s-v2 series
Canada Central 1 Year Reserved ds series
Canada Central 1 Year Reserved e series
Canada Central 1 Year Reserved e-2s series
Canada Central 1 Year Reserved e-32s series
Canada Central 1 Year Reserved e-4s series
Canada Central 1 Year Reserved e-8s series
Canada Central 1 Year Reserved ei series
Canada Central 1 Year Reserved eis series
Canada Central 1 Year Reserved es series
Canada Central 1 Year Reserved f series
Canada Central 1 Year Reserved f1 series
Canada Central 1 Year Reserved f4 series
Canada Central 1 Year Reserved fs series
Canada Central 1 Year Reserved g series
Canada Central 1 Year Reserved gs series
Canada Central 1 Year Reserved ls series
Canada Central 1 Year Reserved m series
Canada Central 1 Year Reserved m-16ms series
Canada Central 1 Year Reserved m-32ms series
Canada Central 1 Year Reserved m-64ms series
Canada Central 1 Year Reserved m-8ms series
Canada Central 1 Year Reserved mls series
Canada Central 1 Year Reserved mm series
Canada Central 1 Year Reserved mms series
Canada Central 1 Year Reserved ms series
Canada Central 1 Year Reserved mts series
Canada Central 3 Year Reserved a series
Canada Central 3 Year Reserved am series
Canada Central 3 Year Reserved d series
Canada Central 3 Year Reserved dc1s-v2 series
Canada Central 3 Year Reserved dc2s-v2 series
Canada Central 3 Year Reserved dc4s-v2 series
Canada Central 3 Year Reserved dc8s-v2 series
Canada Central 3 Year Reserved ds series
Canada Central 3 Year Reserved e series
Canada Central 3 Year Reserved e-2s series
Canada Central 3 Year Reserved e-32s series
Canada Central 3 Year Reserved e-4s series
Canada Central 3 Year Reserved e-8s series
Canada Central 3 Year Reserved e1 series
Canada Central 3 Year Reserved eis series
Canada Central 3 Year Reserved es series
Canada Central 3 Year Reserved f series
Canada Central 3 Year Reserved f1 series
Canada Central 3 Year Reserved f4 series
Canada Central 3 Year Reserved fs series
Canada Central 3 Year Reserved g series
Canada Central 3 Year Reserved gs series
Canada Central 3 Year Reserved ls series
Canada Central 3 Year Reserved m series
Canada Central 3 Year Reserved m-16ms series
Canada Central 3 Year Reserved m-32ms series
Canada Central 3 Year Reserved m-64ms series
Canada Central 3 Year Reserved m-8ms series
Canada Central 3 Year Reserved mls series
Canada Central 3 Year Reserved mms series
Canada Central 3 Year Reserved ms series
Canada Central 3 Year Reserved mts series
Canada East d series
Canada East ds series
Canada East ls series
Canada East m-8ms series
Canada East 1 Year Reserved a series
Canada East 1 Year Reserved am series
Canada East 1 Year Reserved d series
Canada East 1 Year Reserved ds series
Canada East 1 Year Reserved e series
Canada East 1 Year Reserved e-2s series
Canada East 1 Year Reserved e-32s series
Canada East 1 Year Reserved e-4s series
Canada East 1 Year Reserved e-8s series
Canada East 1 Year Reserved e1 series
Canada East 1 Year Reserved eis series
Canada East 1 Year Reserved es series
Canada East 1 Year Reserved f series
Chapter 4  Using the Platform
Reports/Pages

Canada East 1 Year Reserved f1 series
Canada East 1 Year Reserved f4 series
Canada East 1 Year Reserved fs series
Canada East 1 Year Reserved g series
Canada East 1 Year Reserved gs series
Canada East 1 Year Reserved ls series
Canada East 1 Year Reserved m series
Canada East 1 Year Reserved m-16ms series
Canada East 1 Year Reserved m-32ms series
Canada East 1 Year Reserved m-64ms series
Canada East 1 Year Reserved m-8ms series
Canada East 1 Year Reserved mls series
Canada East 1 Year Reserved mm series
Canada East 1 Year Reserved mms series
Canada East 1 Year Reserved ms series
Canada East 1 Year Reserved mts series
Canada East 3 Year Reserved a series
Canada East 3 Year Reserved am series
Canada East 3 Year Reserved d series
Canada East 3 Year Reserved ds series
Canada East 3 Year Reserved e series
Canada East 3 Year Reserved e-2s series
Canada East 3 Year Reserved e-32s series
Canada East 3 Year Reserved e-4s series
Canada East 3 Year Reserved e-8s series
Canada East 3 Year Reserved eis series
Canada East 3 Year Reserved es series
Canada East 3 Year Reserved f series
Canada East 3 Year Reserved f1 series
Canada East 3 Year Reserved f4 series
Canada East 3 Year Reserved fs series
Canada East 3 Year Reserved g series
Canada East 3 Year Reserved gs series
Canada East 3 Year Reserved ls series
Canada East 3 Year Reserved m series
Canada East 3 Year Reserved m-16ms series
Canada East 3 Year Reserved m-32ms series
Canada East 3 Year Reserved m-64ms series
Canada East 3 Year Reserved m-8ms series
Canada East 3 Year Reserved mls series
Canada East 3 Year Reserved mm series
Canada East 3 Year Reserved mms series
Canada East 3 Year Reserved ms series
Canada East 3 Year Reserved mts series
Central India d series
Central India ds series
Central India m-8ms series
Central India 1 Year Reserved a series
Central India 1 Year Reserved am series
Central India 1 Year Reserved d series
Central India 1 Year Reserved ds series
Central India 1 Year Reserved e series
Central India 1 Year Reserved e-2s series
Central India 1 Year Reserved e-32s series
Central India 1 Year Reserved e-4s series
Central India 1 Year Reserved e-8s series
Central India 1 Year Reserved es series
Central India 1 Year Reserved f series
Central India 1 Year Reserved f1 series
Central India 1 Year Reserved f4 series
Central India 1 Year Reserved fs series
Central India 1 Year Reserved h series
Central India 1 Year Reserved m series
Central India 1 Year Reserved m-16ms series
Central India 1 Year Reserved m-32ms series
Central India 1 Year Reserved m-64ms series
Central India 1 Year Reserved m-8ms series
Central India 1 Year Reserved ml series
Central India 1 Year Reserved mm series
Central India 1 Year Reserved mms series
Central India 1 Year Reserved ms series
Central India 1 Year Reserved mts series
Central India 3 Year Reserved a series
Central India 3 Year Reserved am series
Central India 3 Year Reserved d series
Central India 3 Year Reserved ds series
Central India 3 Year Reserved e series
Central India 3 Year Reserved e-2s series
Central India 3 Year Reserved e-32s series
Central India 3 Year Reserved e-4s series
Central India 3 Year Reserved e-8s series
Central India 3 Year Reserved f series
Central India 3 Year Reserved f1 series
Central India 3 Year Reserved f4 series
Central India 3 Year Reserved fs series
Central India 3 Year Reserved h series
Central India 3 Year Reserved m series
Central India 3 Year Reserved m-16ms series
Central India 3 Year Reserved m-32ms series
Central India 3 Year Reserved m-64ms series
Central India 3 Year Reserved m-8ms series
Central India 3 Year Reserved ml series
Central India 3 Year Reserved mm series
Central India 3 Year Reserved mms series
Central India 3 Year Reserved ms series
Central India 3 Year Reserved mts series
Central US d series
Central US ds series
Central US 1 Year Reserved a series
Central US 1 Year Reserved am series
Central US 1 Year Reserved d series
Central US 1 Year Reserved ds series
Central US 1 Year Reserved e series
Central US 1 Year Reserved e-2s series
Central US 1 Year Reserved e-32s series
Central US 1 Year Reserved e-4s series
Central US 1 Year Reserved e-8s series
Central US 1 Year Reserved el series
Central US 1 Year Reserved els series
Central US 1 Year Reserved es series
Central US 1 Year Reserved f series
Central US 1 Year Reserved f1 series
Central US 1 Year Reserved f4 series
Central US 1 Year Reserved fs series
Central US 3 Year Reserved a series
Central US 3 Year Reserved am series
Central US 3 Year Reserved d series
Central US 3 Year Reserved ds series
Central US 3 Year Reserved e series
Central US 3 Year Reserved e-2s series
Central US 3 Year Reserved e-32s series
Central US 3 Year Reserved e-4s series
Central US 3 Year Reserved e-8s series
Central US 3 Year Reserved e1 series
Central US 3 Year Reserved eis series
Central US 3 Year Reserved es series
Central US 3 Year Reserved f series
Central US 3 Year Reserved f1 series
Central US 3 Year Reserved f4 series
Central US 3 Year Reserved fs series
East Asia d series
East Asia ds series
East Asia m series
East Asia m-16ms series
East Asia m-32ms series
East Asia m-64ms series
East Asia m-8ms series
East Asia mls series
East Asia mm series
East Asia mms series
East Asia ms series
East Asia mts series
East Asia 1 Year Reserved a series
East Asia 1 Year Reserved am series
East Asia 1 Year Reserved d series
East Asia 1 Year Reserved ds series
East Asia 1 Year Reserved e series
East Asia 1 Year Reserved e-2s series
East Asia 1 Year Reserved e-32s series
East Asia 1 Year Reserved e-4s series
East Asia 1 Year Reserved e-8s series
East Asia 1 Year Reserved e1 series
East Asia 1 Year Reserved eis series
East Asia 1 Year Reserved es series
East Asia 1 Year Reserved f series
East Asia 1 Year Reserved f1 series
East Asia 1 Year Reserved f4 series
East Asia 1 Year Reserved fs series
East Asia 1 Year Reserved m series
East Asia 1 Year Reserved m-16ms series
East Asia 1 Year Reserved m-32ms series
East Asia 1 Year Reserved m-64ms series
East Asia 1 Year Reserved m-8ms series
East Asia 1 Year Reserved mls series
East Asia 1 Year Reserved mm series
East Asia 1 Year Reserved mms series
East Asia 1 Year Reserved ms series
East Asia 1 Year Reserved mts series
East Asia 3 Year Reserved a series
East Asia 3 Year Reserved am series
East Asia 3 Year Reserved d series
East Asia 3 Year Reserved ds series
East Asia 3 Year Reserved e series
East Asia 3 Year Reserved e-2s series
East Asia 3 Year Reserved e-32s series
East Asia 3 Year Reserved e-4s series
East Asia 3 Year Reserved e-8s series
East Asia 3 Year Reserved ei series
East Asia 3 Year Reserved eis series
East Asia 3 Year Reserved e-2s series
East Asia 3 Year Reserved e-4s series
East Asia 3 Year Reserved e-8s series
East Asia 3 Year Reserved e-16s series
East Asia 3 Year Reserved f series
East Asia 3 Year Reserved f1 series
East Asia 3 Year Reserved f4 series
East Asia 3 Year Reserved fs series
East Asia 3 Year Reserved m series
East Asia 3 Year Reserved m-16ms series
East Asia 3 Year Reserved m-32ms series
East Asia 3 Year Reserved m-64ms series
East Asia 3 Year Reserved m-8ms series
East Asia 3 Year Reserved mls series
East Asia 3 Year Reserved mm series
East Asia 3 Year Reserved mm series
East Asia 3 Year Reserved ms series
East Asia 3 Year Reserved mts series
East US d series
East US da series
East US das series
East US ds series
East US ea series
East US eas series
East US m-8ms series
East US mms series
East US ms series
East US 1 Year Reserved a series
East US 1 Year Reserved am series
East US 1 Year Reserved d series
East US 1 Year Reserved da series
East US 1 Year Reserved das series
East US 1 Year Reserved dc2s series
East US 1 Year Reserved dc4s series
East US 1 Year Reserved ds series
East US 1 Year Reserved e series
East US 1 Year Reserved e-2s series
East US 1 Year Reserved e-32s series
East US 1 Year Reserved e-4s series
East US 1 Year Reserved e-8s series
East US 1 Year Reserved ea series
East US 1 Year Reserved eas series
East US 1 Year Reserved ei series
East US 1 Year Reserved eis series
East US 1 Year Reserved es series
East US 1 Year Reserved f series
East US 1 Year Reserved f1 series
East US 1 Year Reserved f4 series
East US 1 Year Reserved fs series
East US 1 Year Reserved h series
East US 1 Year Reserved hc44rs series
East US 1 Year Reserved l series
East US 1 Year Reserved ls series
East US 1 Year Reserved m series
East US 1 Year Reserved m-16ms series
East US 1 Year Reserved m-32ms series
East US 1 Year Reserved m-64ms series
East US 1 Year Reserved m-8ms series
East US 1 Year Reserved mls series
East US 1 Year Reserved mm series
East US 1 Year Reserved mms series
East US 1 Year Reserved ms series
East US 1 Year Reserved mts series
East US 2 d series
East US 2 da series
East US 2 das series
East US 2 ds series
East US 2 ea series
East US 2 eas series
East US 2 ls series
East US 2 m-8ms series
East US 2 mms series
East US 2 ms series
East US 2 1 Year Reserved a series
East US 2 1 Year Reserved am series
East US 2 1 Year Reserved d series
East US 2 1 Year Reserved da series
East US 2 1 Year Reserved das series
East US 2 1 Year Reserved ds series
East US 2 1 Year Reserved e series
East US 2 1 Year Reserved e-2s series
East US 2 1 Year Reserved e-32s series
East US 2 1 Year Reserved e-4s series
East US 2 1 Year Reserved e-8s series
East US 2 1 Year Reserved ea series
East US 2 1 Year Reserved eas series
East US 2 1 Year Reserved ei series
East US 2 1 Year Reserved eis series
East US 2 1 Year Reserved es series
East US 2 1 Year Reserved f series
East US 2 1 Year Reserved f1 series
East US 2 1 Year Reserved f4 series
East US 2 1 Year Reserved fs series
East US 2 1 Year Reserved g series
East US 2 1 Year Reserved gs series
East US 2 1 Year Reserved l series
East US 2 1 Year Reserved ls series
East US 2 1 Year Reserved m series
East US 2 1 Year Reserved m-16ms series
East US 2 1 Year Reserved m-32ms series
East US 2 1 Year Reserved m-64ms series
East US 2 1 Year Reserved m-8ms series
East US 2 1 Year Reserved mls series
East US 2 1 Year Reserved mm series
East US 2 1 Year Reserved mms series
East US 2 1 Year Reserved ms series
East US 2 1 Year Reserved mts series
East US 2 3 Year Reserved a series
East US 2 3 Year Reserved am series
East US 2 3 Year Reserved d series
East US 2 3 Year Reserved da series
East US 2 3 Year Reserved das series
East US 2 3 Year Reserved ds series
East US 2 3 Year Reserved e series
East US 2 3 Year Reserved e-2s series
East US 2 3 Year Reserved e-32s series
East US 2 3 Year Reserved e-4s series
East US 2 3 Year Reserved e-8s series
East US 2 3 Year Reserved ea series
East US 2 3 Year Reserved eas series
East US 2 3 Year Reserved ei series
East US 2 3 Year Reserved eis series
East US 2 3 Year Reserved es series
East US 2 3 Year Reserved f series
East US 2 3 Year Reserved f1 series
East US 2 3 Year Reserved f4 series
East US 2 3 Year Reserved fs series
East US 2 3 Year Reserved g series
East US 2 3 Year Reserved gs series
East US 2 3 Year Reserved l series
East US 2 3 Year Reserved ls series
East US 2 3 Year Reserved m series
East US 2 3 Year Reserved m-16ms series
East US 2 3 Year Reserved m-32ms series
East US 2 3 Year Reserved m-64ms series
East US 2 3 Year Reserved m-8ms series
East US 2 3 Year Reserved mls series
East US 2 3 Year Reserved mm series
East US 2 3 Year Reserved mms series
East US 2 3 Year Reserved ms series
East US 2 3 Year Reserved mts series
East US 3 Year Reserved a series
East US 3 Year Reserved am series
East US 3 Year Reserved d series
East US 3 Year Reserved da series
East US 3 Year Reserved das series
East US 3 Year Reserved dc2s series
East US 3 Year Reserved dc4s series
East US 3 Year Reserved ds series
East US 3 Year Reserved e series
East US 3 Year Reserved e-2s series
East US 3 Year Reserved e-32s series
East US 3 Year Reserved e-4s series
East US 3 Year Reserved e-8s series
East US 3 Year Reserved ea series
East US 3 Year Reserved eas series
East US 3 Year Reserved ei series
East US 3 Year Reserved eis series
East US 3 Year Reserved es series
East US 3 Year Reserved es series
East US 3 Year Reserved f series
East US 3 Year Reserved f1 series
East US 3 Year Reserved f4 series
East US 3 Year Reserved fs series
East US 3 Year Reserved h series
East US 3 Year Reserved hc44rs series
East US 3 Year Reserved l series
East US 3 Year Reserved ls series
East US 3 Year Reserved m series
East US 3 Year Reserved m-16ms series
East US 3 Year Reserved m-32ms series
East US 3 Year Reserved m-64ms series
East US 3 Year Reserved m-8ms series
East US 3 Year Reserved mls series
East US 3 Year Reserved mm series
East US 3 Year Reserved mms series
East US 3 Year Reserved ms series
East US 3 Year Reserved mts series
France Central d series
France Central ds series
France Central e series
France Central e-2s series
France Central e-32s series
France Central e-4s series
France Central e-8s series
France Central es series
France Central m-8ms series
France Central 1 Year Reserved a series
France Central 1 Year Reserved am series
France Central 1 Year Reserved d series
France Central 1 Year Reserved ds series
France Central 1 Year Reserved e series
France Central 1 Year Reserved e-2s series
France Central 1 Year Reserved e-32s series
France Central 1 Year Reserved e-4s series
France Central 1 Year Reserved e-8s series
France Central 1 Year Reserved ei series
France Central 1 Year Reserved el series
France Central 1 Year Reserved es series
France Central 1 Year Reserved f series
France Central 1 Year Reserved f1 series
France Central 1 Year Reserved f4 series
France Central 1 Year Reserved fs series
France Central 1 Year Reserved m series
France Central 1 Year Reserved m-16ms series
France Central 1 Year Reserved m-32ms series
France Central 1 Year Reserved m-64ms series
France Central 1 Year Reserved m-8ms series
France Central 1 Year Reserved mls series
France Central 1 Year Reserved mm series
France Central 1 Year Reserved mms series
France Central 1 Year Reserved ms series
France Central 1 Year Reserved mts series
France Central 3 Year Reserved a series
France Central 3 Year Reserved am series
France Central 3 Year Reserved d series
France Central 3 Year Reserved ds series
France Central 3 Year Reserved e series
France Central 3 Year Reserved e-2s series
France Central 3 Year Reserved e-32s series
France Central 3 Year Reserved e-4s series
France Central 3 Year Reserved e-8s series
France Central 3 Year Reserved ei series
France Central 3 Year Reserved eis series
France Central 3 Year Reserved es series
France Central 3 Year Reserved ei series
France South 3 Year Reserved d series
France South 3 Year Reserved ds series
France South 3 Year Reserved e series
France South 3 Year Reserved e-2s series
France South 3 Year Reserved e-32s series
France South 3 Year Reserved e-4s series
France South 3 Year Reserved e-8s series
France South 3 Year Reserved a series
France South 3 Year Reserved am series
France South 3 Year Reserved d series
France South 3 Year Reserved ds series
France South 3 Year Reserved e series
France South 3 Year Reserved e-2s series
France South 3 Year Reserved e-32s series
France South 3 Year Reserved e-4s series
France South 3 Year Reserved e-8s series
France South 3 Year Reserved a series
France South 3 Year Reserved am series
France South 3 Year Reserved d series
France South 3 Year Reserved ds series
France South 3 Year Reserved e series
France South 3 Year Reserved e-2s series
France South 3 Year Reserved e-32s series
France South 3 Year Reserved e-4s series
France South 3 Year Reserved e-8s series
France South 3 Year Reserved ei series
France South 3 Year Reserved eis series
France South 3 Year Reserved es series
France South 3 Year Reserved f series
France South 3 Year Reserved f1 series
France South 3 Year Reserved f4 series
France South 3 Year Reserved fs series
Germany Central d series
Germany Central ds series
Germany Central e series
Germany Central es series
Germany Central f series
Germany Central fs series
Germany Central ls series
Germany Central 1 Year Reserved a series
Germany Central 1 Year Reserved am series
Germany Central 1 Year Reserved d series
Germany Central 1 Year Reserved ds series
Germany Central 1 Year Reserved e series
Germany Central 1 Year Reserved e-2s series
Germany Central 1 Year Reserved e-32s series
Germany Central 1 Year Reserved e-4s series
Germany Central 1 Year Reserved e-8s series
Germany Central 1 Year Reserved ei series
Germany Central 1 Year Reserved eis series
Germany Central 1 Year Reserved es series
Germany Central 1 Year Reserved f series
Germany Central 1 Year Reserved f1 series
Germany Central 1 Year Reserved f4 series
Germany Central 1 Year Reserved fs series
Germany Central 1 Year Reserved g series
Germany Central 1 Year Reserved gs series
Germany Central 1 Year Reserved ls series
Germany Northeast d series
Germany Northeast ds series
Germany Northeast e series
Germany Northeast es series
Germany Northeast g series
Germany Northeast gs series
Germany Northeast 1 Year Reserved a series
Germany Northeast 1 Year Reserved am series
Germany Northeast 1 Year Reserved d series
Germany Northeast 1 Year Reserved ds series
Germany Northeast 1 Year Reserved e series
Germany Northeast 1 Year Reserved e-2s series
Germany Northeast 1 Year Reserved e-32s series
Germany Northeast 1 Year Reserved e-4s series
Germany Northeast 1 Year Reserved e-8s series
Germany Northeast 1 Year Reserved ei series
Germany Northeast 1 Year Reserved eis series
Germany Northeast 1 Year Reserved es series
Germany Northeast 1 Year Reserved f series
Germany Northeast 1 Year Reserved f1 series
Germany Northeast 1 Year Reserved f4 series
Germany Northeast 1 Year Reserved fs series
Germany Northeast 1 Year Reserved g series
Germany Northeast 1 Year Reserved gs series
Japan East d series
Japan East ds series
Japan East hC44rs series
Japan East lS series
Japan East m-8ms series
Japan East 1 Year Reserved a series
Japan East 1 Year Reserved am series
Japan East 1 Year Reserved d series
Japan East 1 Year Reserved ds series
Japan East 1 Year Reserved e series
Japan East 1 Year Reserved e-2s series
Japan East 1 Year Reserved e-32s series
Japan East 1 Year Reserved e-4s series
Japan East 1 Year Reserved e-8s series
Japan East 1 Year Reserved el series
Japan East 1 Year Reserved els series
Japan East 1 Year Reserved es series
Japan East 1 Year Reserved f series
Japan East 1 Year Reserved f1 series
Japan East 1 Year Reserved f4 series
Japan East 1 Year Reserved fs series
Japan East 1 Year Reserved g series
Japan East 1 Year Reserved gs series
Japan East 1 Year Reserved h series
Japan East 1 Year Reserved hC44rs series
Japan East 1 Year Reserved lS series
Japan East 1 Year Reserved m series
Japan East 1 Year Reserved m-16ms series
Japan East 1 Year Reserved m-32ms series
Japan East 1 Year Reserved m-64ms series
Japan East 1 Year Reserved m-8ms series
Japan East 1 Year Reserved mls series
Japan East 1 Year Reserved mm series
Japan East 1 Year Reserved mms series
Japan East 1 Year Reserved mss series
Japan East 1 Year Reserved mts series
Japan East 3 Year Reserved a series
Japan East 3 Year Reserved am series
Japan East 3 Year Reserved ds series
Japan East 3 Year Reserved e series
Japan East 3 Year Reserved e-2s series
Japan East 3 Year Reserved e-32s series
Japan East 3 Year Reserved e-4s series
Japan East 3 Year Reserved e-8s series
Japan East 3 Year Reserved el series
Japan East 3 Year Reserved els series
Japan East 3 Year Reserved es series
Japan East 3 Year Reserved f series
Japan East 3 Year Reserved f1 series
Japan East 3 Year Reserved f4 series
Japan East 3 Year Reserved fs series
Japan East 3 Year Reserved g series
Japan East 3 Year Reserved gs series
Japan East 3 Year Reserved h series
Japan East 3 Year Reserved hc44rs series
Japan East 3 Year Reserved ls series
Japan East 3 Year Reserved m series
Japan East 3 Year Reserved m-16ms series
Japan East 3 Year Reserved m-32ms series
Japan East 3 Year Reserved m-64ms series
Japan East 3 Year Reserved m-8ms series
Japan East 3 Year Reserved mls series
Japan East 3 Year Reserved mm series
Japan East 3 Year Reserved mms series
Japan East 3 Year Reserved ms series
Japan East 3 Year Reserved mts series
Japan West d series
Japan West ds series
Japan West m-8ms series
Japan West 1 Year Reserved a series
Japan West 1 Year Reserved am series
Japan West 1 Year Reserved d series
Japan West 1 Year Reserved ds series
Japan West 1 Year Reserved e series
Japan West 1 Year Reserved e-2s series
Japan West 1 Year Reserved e-32s series
Japan West 1 Year Reserved e-4s series
Japan West 1 Year Reserved e-8s series
Japan West 1 Year Reserved el series
Japan West 1 Year Reserved els series
Japan West 1 Year Reserved es series
Japan West 1 Year Reserved f series
Japan West 1 Year Reserved f1 series
Japan West 1 Year Reserved f4 series
Japan West 1 Year Reserved fs series
Japan West 1 Year Reserved m series
Japan West 1 Year Reserved m-16ms series
Japan West 1 Year Reserved m-32ms series
Japan West 1 Year Reserved m-64ms series
Japan West 1 Year Reserved m-8ms series
Japan West 1 Year Reserved mls series
Japan West 1 Year Reserved mm series
Japan West 1 Year Reserved mms series
Japan West 1 Year Reserved ms series
Japan West 1 Year Reserved mts series
Japan West 3 Year Reserved a series
Japan West 3 Year Reserved am series
Japan West 3 Year Reserved d series
Japan West 3 Year Reserved ds series
Japan West 3 Year Reserved e series
Japan West 3 Year Reserved e-2s series
Japan West 3 Year Reserved e-32s series
Japan West 3 Year Reserved e-4s series
Japan West 3 Year Reserved e-8s series
Japan West 3 Year Reserved el series
Japan West 3 Year Reserved els series
Japan West 3 Year Reserved es series
Japan West 3 Year Reserved f series
Japan West 3 Year Reserved f1 series
Chapter 4  Using the Platform
Reports/Pages

Japan West 3 Year Reserved f4 series
Japan West 3 Year Reserved fs series
Japan West 3 Year Reserved m series
Japan West 3 Year Reserved m-16ms series
Japan West 3 Year Reserved m-32ms series
Japan West 3 Year Reserved m-64ms series
Japan West 3 Year Reserved m-8ms series
Japan West 3 Year Reserved mls series
Japan West 3 Year Reserved mm series
Japan West 3 Year Reserved mms series
Japan West 3 Year Reserved ms series
Japan West 3 Year Reserved mts series
Korea Central d series
Korea Central ds series
Korea Central m-8ms series
Korea Central mms series
Korea Central ms series
Korea Central 1 Year Reserved a series
Korea Central 1 Year Reserved am series
Korea Central 1 Year Reserved d series
Korea Central 1 Year Reserved ds series
Korea Central 1 Year Reserved e series
Korea Central 1 Year Reserved e-2s series
Korea Central 1 Year Reserved e-32s series
Korea Central 1 Year Reserved e-4s series
Korea Central 1 Year Reserved e-8s series
Korea Central 1 Year Reserved ei series
Korea Central 1 Year Reserved eis series
Korea Central 1 Year Reserved es series
Korea Central 1 Year Reserved f series
Korea Central 1 Year Reserved f1 series
Korea Central 1 Year Reserved f4 series
Korea Central 1 Year Reserved fs series
Korea Central 1 Year Reserved m series
Korea Central 1 Year Reserved m-16ms series
Korea Central 1 Year Reserved m-32ms series
Korea Central 1 Year Reserved m-64ms series
Korea Central 1 Year Reserved m-8ms series
Korea Central 1 Year Reserved mls series
Korea Central 1 Year Reserved mm series
Korea Central 1 Year Reserved mms series
Korea Central 1 Year Reserved ms series
Korea Central 1 Year Reserved mts series
Korea Central 3 Year Reserved a series
Korea Central 3 Year Reserved am series
Korea Central 3 Year Reserved d series
Korea Central 3 Year Reserved ds series
Korea Central 3 Year Reserved e series
Korea Central 3 Year Reserved e-2s series
Korea Central 3 Year Reserved e-32s series
Korea Central 3 Year Reserved e-4s series
Korea Central 3 Year Reserved e-8s series
Korea Central 3 Year Reserved ei series
Korea Central 3 Year Reserved eis series
Korea Central 3 Year Reserved es series
Korea Central 3 Year Reserved f series
Korea Central 3 Year Reserved f1 series
Korea Central 3 Year Reserved f4 series
Korea Central 3 Year Reserved fs series
Korea Central 3 Year Reserved f1 series
Korea Central 3 Year Reserved f4 series
Korea Central 3 Year Reserved fs series
Korea Central 3 Year Reserved m series
Korea Central 3 Year Reserved m-16ms series
Korea Central 3 Year Reserved m-32ms series
Korea Central 3 Year Reserved m-64ms series
Korea Central 3 Year Reserved m-8ms series
Korea Central 3 Year Reserved mls series
Korea Central 3 Year Reserved mm series
Korea Central 3 Year Reserved mms series
Korea Central 3 Year Reserved ms series
Korea Central 3 Year Reserved mts series
Korea South d series
Korea South ds series
Korea South m-8ms series
Korea South 1 Year Reserved a series
Korea South 1 Year Reserved am series
Korea South 1 Year Reserved d series
Korea South 1 Year Reserved ds series
Korea South 1 Year Reserved e series
Korea South 1 Year Reserved e-2s series
Korea South 1 Year Reserved e-32s series
Korea South 1 Year Reserved e-4s series
Korea South 1 Year Reserved e-8s series
Korea South 1 Year Reserved ei series
Korea South 1 Year Reserved eis series
Korea South 1 Year Reserved es series
Korea South 1 Year Reserved f series
Korea South 1 Year Reserved f1 series
Korea South 1 Year Reserved f4 series
Korea South 1 Year Reserved fs series
Korea South 1 Year Reserved m series
Korea South 1 Year Reserved m-16ms series
Korea South 1 Year Reserved m-32ms series
Korea South 1 Year Reserved m-64ms series
Korea South 1 Year Reserved m-8ms series
Korea South 1 Year Reserved mls series
Korea South 1 Year Reserved mm series
Korea South 1 Year Reserved mms series
Korea South 1 Year Reserved ms series
Korea South 1 Year Reserved mts series
Korea South 3 Year Reserved a series
Korea South 3 Year Reserved am series
Korea South 3 Year Reserved d series
Korea South 3 Year Reserved ds series
Korea South 3 Year Reserved e series
Korea South 3 Year Reserved e-2s series
Korea South 3 Year Reserved e-32s series
Korea South 3 Year Reserved e-4s series
Korea South 3 Year Reserved e-8s series
Korea South 3 Year Reserved ei series
Korea South 3 Year Reserved eis series
Korea South 3 Year Reserved es series
Korea South 3 Year Reserved f series
Korea South 3 Year Reserved f1 series
Korea South 3 Year Reserved f4 series
Korea South 3 Year Reserved fs series
Korea South 3 Year Reserved m series
Korea South 3 Year Reserved m-16ms series
Korea South 3 Year Reserved m-32ms series
Korea South 3 Year Reserved m-64ms series
Korea South 3 Year Reserved m-8ms series
Korea South 3 Year Reserved mls series
Korea South 3 Year Reserved mm series
Korea South 3 Year Reserved mms series
Korea South 3 Year Reserved ms series
Korea South 3 Year Reserved mts series
North Central US d series
North Central US ds series
North Central US 1 Year Reserved a series
North Central US 1 Year Reserved am series
North Central US 1 Year Reserved d series
North Central US 1 Year Reserved ds series
North Central US 1 Year Reserved e series
North Central US 1 Year Reserved e-2s series
North Central US 1 Year Reserved e-32s series
North Central US 1 Year Reserved e-4s series
North Central US 1 Year Reserved e-8s series
North Central US 1 Year Reserved ei series
North Central US 1 Year Reserved f series
North Central US 1 Year Reserved f1 series
North Central US 1 Year Reserved f4 series
North Central US 1 Year Reserved fs series
North Central US 1 Year Reserved h series
North Central US 3 Year Reserved a series
North Central US 3 Year Reserved am series
North Central US 3 Year Reserved d series
North Central US 3 Year Reserved ds series
North Central US 3 Year Reserved e series
North Central US 3 Year Reserved e-2s series
North Central US 3 Year Reserved e-32s series
North Central US 3 Year Reserved e-4s series
North Central US 3 Year Reserved e-8s series
North Central US 3 Year Reserved ei series
North Central US 3 Year Reserved f series
North Central US 3 Year Reserved f1 series
North Central US 3 Year Reserved f4 series
North Central US 3 Year Reserved fs series
North Central US 3 Year Reserved h series
North Europe d series
North Europe da series
North Europe das series
North Europe ds series
North Europe ea series
North Europe eas series
North Europe m-8ms series
North Europe mms series
North Europe ms series
North Europe 1 Year Reserved a series
North Europe 1 Year Reserved am series
North Europe 1 Year Reserved d series
North Europe 1 Year Reserved da series
North Europe 1 Year Reserved das series
North Europe 1 Year Reserved ds series
North Europe 1 Year Reserved e series
North Europe 1 Year Reserved e-2s series
North Europe 1 Year Reserved e-32s series
North Europe 1 Year Reserved e-4s series
North Europe 1 Year Reserved e-8s series
North Europe 1 Year Reserved ea series
North Europe 1 Year Reserved eas series
North Europe 1 Year Reserved el series
North Europe 1 Year Reserved eis series
North Europe 1 Year Reserved es series
North Europe 1 Year Reserved f series
North Europe 1 Year Reserved f1 series
North Europe 1 Year Reserved f4 series
North Europe 1 Year Reserved fs series
North Europe 1 Year Reserved h series
North Europe 1 Year Reserved l series
North Europe 1 Year Reserved ls series
North Europe 1 Year Reserved m series
North Europe 1 Year Reserved m-16ms series
North Europe 1 Year Reserved m-32ms series
North Europe 1 Year Reserved m-64ms series
North Europe 1 Year Reserved m-8ms series
North Europe 1 Year Reserved mls series
North Europe 1 Year Reserved mm series
North Europe 1 Year Reserved mms series
North Europe 1 Year Reserved ms series
North Europe 1 Year Reserved mts series
North Europe 3 Year Reserved a series
North Europe 3 Year Reserved am series
North Europe 3 Year Reserved d series
North Europe 3 Year Reserved da series
North Europe 3 Year Reserved das series
North Europe 3 Year Reserved ds series
North Europe 3 Year Reserved e series
North Europe 3 Year Reserved e-2s series
North Europe 3 Year Reserved e-32s series
North Europe 3 Year Reserved e-4s series
North Europe 3 Year Reserved e-8s series
North Europe 3 Year Reserved ea series
North Europe 3 Year Reserved eas series
North Europe 3 Year Reserved el series
North Europe 3 Year Reserved eis series
North Europe 3 Year Reserved es series
North Europe 3 Year Reserved f series
North Europe 3 Year Reserved f1 series
North Europe 3 Year Reserved f4 series
North Europe 3 Year Reserved fs series
North Europe 3 Year Reserved h series
North Europe 3 Year Reserved l series
North Europe 3 Year Reserved ls series
North Europe 3 Year Reserved m series
North Europe 3 Year Reserved m-16ms series
North Europe 3 Year Reserved m-32ms series
North Europe 3 Year Reserved m-64ms series
North Europe 3 Year Reserved m-8ms series
North Europe 3 Year Reserved ml series
North Europe 3 Year Reserved mm series
North Europe 3 Year Reserved mms series
North Europe 3 Year Reserved ms series
North Europe 3 Year Reserved mts series
South Central US d series
South Central US ds series
South Central US hc44rs series
South Central US 1 series
South Central US ls series
South Central US m-8ms series
South Central US mms series
South Central US ms series
South Central US 1 Year Reserved a series
South Central US 1 Year Reserved am series
South Central US 1 Year Reserved d series
South Central US 1 Year Reserved ds series
South Central US 1 Year Reserved e series
South Central US 1 Year Reserved e-2s series
South Central US 1 Year Reserved e-32s series
South Central US 1 Year Reserved e-4s series
South Central US 1 Year Reserved e-8s series
South Central US 1 Year Reserved ei series
South Central US 1 Year Reserved eis series
South Central US 1 Year Reserved es series
South Central US 1 Year Reserved f series
South Central US 1 Year Reserved f1 series
South Central US 1 Year Reserved f4 series
South Central US 1 Year Reserved fs series
South Central US 1 Year Reserved h series
South Central US 1 Year Reserved hc44rs series
South Central US 1 Year Reserved l series
South Central US 1 Year Reserved ls series
South Central US 1 Year Reserved m series
South Central US 1 Year Reserved m-16ms series
South Central US 1 Year Reserved m-32ms series
South Central US 1 Year Reserved m-64ms series
South Central US 1 Year Reserved m-8ms series
South Central US 1 Year Reserved mls series
South Central US 1 Year Reserved mm series
South Central US 1 Year Reserved mms series
South Central US 1 Year Reserved ms series
South Central US 1 Year Reserved mts series
South Central US 3 Year Reserved a series
South Central US 3 Year Reserved am series
South Central US 3 Year Reserved d series
South Central US 3 Year Reserved ds series
South Central US 3 Year Reserved e series
South Central US 3 Year Reserved e-2s series
South Central US 3 Year Reserved e-32s series
South Central US 3 Year Reserved e-4s series
South Central US 3 Year Reserved e-8s series
South Central US 3 Year Reserved ei series
South Central US 3 Year Reserved eis series
South Central US 3 Year Reserved es series
South Central US 3 Year Reserved f series
South Central US 3 Year Reserved f1 series
South Central US 3 Year Reserved f4 series
South Central US 3 Year Reserved fs series
South Central US 3 Year Reserved h series
South Central US 3 Year Reserved hc44rs series
South Central US 3 Year Reserved m series
South Central US 3 Year Reserved m-16ms series
South Central US 3 Year Reserved m-32ms series
South Central US 3 Year Reserved m-64ms series
South Central US 3 Year Reserved m-8ms series
South Central US 3 Year Reserved mls series
South Central US 3 Year Reserved mm series
South Central US 3 Year Reserved mms series
South Central US 3 Year Reserved ms series
South Central US 3 Year Reserved mts series
South India d series
South India ds series
South India m-8ms series
South India 1 Year Reserved a series
South India 1 Year Reserved am series
South India 1 Year Reserved d series
South India 1 Year Reserved ds series
South India 1 Year Reserved e series
South India 1 Year Reserved e-2s series
South India 1 Year Reserved e-32s series
South India 1 Year Reserved e-4s series
South India 1 Year Reserved e-8s series
South India 1 Year Reserved ei series
South India 1 Year Reserved eis series
South India 1 Year Reserved es series
South India 1 Year Reserved f series
South India 1 Year Reserved f1 series
South India 1 Year Reserved f4 series
South India 1 Year Reserved fs series
South India 1 Year Reserved m series
South India 1 Year Reserved m-16ms series
South India 1 Year Reserved m-32ms series
South India 1 Year Reserved m-64ms series
South India 1 Year Reserved m-8ms series
South India 1 Year Reserved mls series
South India 1 Year Reserved mm series
South India 1 Year Reserved mms series
South India 1 Year Reserved ms series
South India 1 Year Reserved mts series
South India 3 Year Reserved a series
South India 3 Year Reserved am series
South India 3 Year Reserved d series
South India 3 Year Reserved ds series
South India 3 Year Reserved e series
South India 3 Year Reserved e-2s series
South India 3 Year Reserved e-32s series
South India 3 Year Reserved e-4s series
South India 3 Year Reserved e-8s series
South India 3 Year Reserved ei series
South India 3 Year Reserved eis series
South India 3 Year Reserved es series
South India 3 Year Reserved f series
South India 3 Year Reserved f1 series
South India 3 Year Reserved f4 series
South India 3 Year Reserved fs series
South India 3 Year Reserved m series
South India 3 Year Reserved m-16ms series
South India 3 Year Reserved m-32ms series
South India 3 Year Reserved m-64ms series
South India 3 Year Reserved m-8ms series
South India 3 Year Reserved mls series
South India 3 Year Reserved mm series
South India 3 Year Reserved mms series
South India 3 Year Reserved ms series
South India 3 Year Reserved mts series
Southeast Asia d series
Southeast Asia da series
Southeast Asia das series
Southeast Asia ea series
Southeast Asia eas series
Southeast Asia ls series
Southeast Asia m-8ms series
Southeast Asia mms series
Southeast Asia ms series
Southeast Asia 1 Year Reserved a series
Southeast Asia 1 Year Reserved am series
Southeast Asia 1 Year Reserved d series
Southeast Asia 1 Year Reserved da series
Southeast Asia 1 Year Reserved das series
Southeast Asia 1 Year Reserved ds series
Southeast Asia 1 Year Reserved e series
Southeast Asia 1 Year Reserved e-2s series
Southeast Asia 1 Year Reserved e-32s series
Southeast Asia 1 Year Reserved e-4s series
Southeast Asia 1 Year Reserved e-8s series
Southeast Asia 1 Year Reserved ea series
Southeast Asia 1 Year Reserved eas series
Southeast Asia 1 Year Reserved ei series
Southeast Asia 1 Year Reserved eis series
Southeast Asia 1 Year Reserved es series
Southeast Asia 1 Year Reserved f series
Southeast Asia 1 Year Reserved f1 series
Southeast Asia 1 Year Reserved f4 series
Southeast Asia 1 Year Reserved fs series
Southeast Asia 1 Year Reserved g series
Southeast Asia 1 Year Reserved gs series
Southeast Asia 1 Year Reserved h series
Southeast Asia 1 Year Reserved l series
Southeast Asia 1 Year Reserved ls series
Southeast Asia 1 Year Reserved m series
Southeast Asia 1 Year Reserved m-16ms series
Southeast Asia 1 Year Reserved m-32ms series
Southeast Asia 1 Year Reserved m-64ms series
Southeast Asia 1 Year Reserved m-8ms series
Southeast Asia 1 Year Reserved mls series
Southeast Asia 1 Year Reserved ms series
Southeast Asia 1 Year Reserved mts series
Southeast Asia 1 Year Reserved ms series
Southeast Asia 1 Year Reserved m-16ms series
Southeast Asia 1 Year Reserved m-32ms series
Southeast Asia 1 Year Reserved m-64ms series
Southeast Asia 1 Year Reserved m-8ms series
Southeast Asia 1 Year Reserved mm series
Southeast Asia 1 Year Reserved mms series
Southeast Asia 1 Year Reserved ms series
Southeast Asia 1 Year Reserved mts series
Southeast Asia 3 Year Reserved a series
Southeast Asia 3 Year Reserved am series
Southeast Asia 3 Year Reserved d series
Southeast Asia 3 Year Reserved da series
Southeast Asia 3 Year Reserved das series
Southeast Asia 3 Year Reserved ds series
Southeast Asia 3 Year Reserved e series
Southeast Asia 3 Year Reserved e-2s series
Southeast Asia 3 Year Reserved e-32s series
Southeast Asia 3 Year Reserved e-4s series
Southeast Asia 3 Year Reserved e-8s series
Southeast Asia 3 Year Reserved ea series
Southeast Asia 3 Year Reserved eas series
Southeast Asia 3 Year Reserved ei series
Southeast Asia 3 Year Reserved eis series
Southeast Asia 3 Year Reserved es series
Southeast Asia 3 Year Reserved f series
Southeast Asia 3 Year Reserved f1 series
Southeast Asia 3 Year Reserved f4 series
Southeast Asia 3 Year Reserved fs series
Southeast Asia 3 Year Reserved g series
Southeast Asia 3 Year Reserved gs series
Southeast Asia 3 Year Reserved h series
Southeast Asia 3 Year Reserved l series
Southeast Asia 3 Year Reserved ls series
Southeast Asia 3 Year Reserved m series
Southeast Asia 3 Year Reserved m-16ms series
Southeast Asia 3 Year Reserved m-32ms series
Southeast Asia 3 Year Reserved m-64ms series
Southeast Asia 3 Year Reserved m-8ms series
Southeast Asia 3 Year Reserved mls series
Southeast Asia 3 Year Reserved mm series
Southeast Asia 3 Year Reserved mms series
Southeast Asia 3 Year Reserved ms series
Southeast Asia 3 Year Reserved mts series
Southeast Asia 3 Year Reserved mts series
UK South d series
UK South dc1s-v2 series
UK South dc2s-v2 series
UK South dc4s-v2 series
UK South dc8s-v2 series
UK South ds series
UK South ls series
UK South m-8ms series
UK South mms series
UK South ms series
UK South 1 Year Reserved a series
UK South 1 Year Reserved am series
UK South 1 Year Reserved d series
UK South 1 Year Reserved dc1s-v2 series
UK South 1 Year Reserved dc2s-v2 series
UK South 1 Year Reserved dc4s-v2 series
UK South 1 Year Reserved dc8s-v2 series
UK South 1 Year Reserved ds series
UK South 1 Year Reserved e series
UK South 1 Year Reserved e-2s series
UK South 1 Year Reserved e-32s series
UK South 1 Year Reserved e-4s series
UK South 1 Year Reserved e-8s series
UK South 1 Year Reserved ei series
UK South 1 Year Reserved eis series
UK South 1 Year Reserved es series
UK South 1 Year Reserved f series
UK South 1 Year Reserved f1 series
UK South 1 Year Reserved f4 series
UK South 1 Year Reserved fs series
UK South 1 Year Reserved g series
UK South 1 Year Reserved gs series
UK South 1 Year Reserved h series
UK South 1 Year Reserved ls series
UK South 1 Year Reserved m series
UK South 1 Year Reserved m-16ms series
UK South 1 Year Reserved m-32ms series
UK South 1 Year Reserved m-64ms series
UK South 1 Year Reserved m-8ms series
UK South 1 Year Reserved mls series
UK South 1 Year Reserved mm series
UK South 1 Year Reserved mms series
UK South 1 Year Reserved ms series
UK South 1 Year Reserved mts series
UK South 3 Year Reserved a series
UK South 3 Year Reserved am series
UK South 3 Year Reserved d series
UK South 3 Year Reserved dc1s-v2 series
UK South 3 Year Reserved dc2s-v2 series
UK South 3 Year Reserved dc4s-v2 series
UK South 3 Year Reserved dc8s-v2 series
UK South 3 Year Reserved ds series
UK South 3 Year Reserved e series
UK South 3 Year Reserved e-2s series
UK South 3 Year Reserved e-32s series
UK South 3 Year Reserved e-4s series
UK South 3 Year Reserved e-8s series
UK South 3 Year Reserved ei series
UK South 3 Year Reserved eis series
UK South 3 Year Reserved es series
UK South 3 Year Reserved f series
UK South 3 Year Reserved f1 series
UK South 3 Year Reserved f4 series
UK South 3 Year Reserved fs series
UK South 3 Year Reserved g series
UK South 3 Year Reserved gs series
UK South 3 Year Reserved h series
UK South 3 Year Reserved ls series
<table>
<thead>
<tr>
<th>Subscription Plan</th>
<th>Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK South 3 Year Reserved m series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved m-16ms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved m-32ms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved m-64ms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved m-8ms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved mls series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved mm series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved mms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved ms series</td>
<td></td>
</tr>
<tr>
<td>UK South 3 Year Reserved mts series</td>
<td></td>
</tr>
<tr>
<td>UK West d series</td>
<td></td>
</tr>
<tr>
<td>UK West ds series</td>
<td></td>
</tr>
<tr>
<td>UK West f series</td>
<td></td>
</tr>
<tr>
<td>UK West fs series</td>
<td></td>
</tr>
<tr>
<td>UK West m-8ms series</td>
<td></td>
</tr>
<tr>
<td>UK West mms series</td>
<td></td>
</tr>
<tr>
<td>UK West ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved a series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved am series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved d series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved ds series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved e series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved e-2s series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved e-32s series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved e-4s series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved e-8s series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved el series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved els series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved es series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved f series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved f1 series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved f4 series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved fs series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved m series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved m-16ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved m-32ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved m-64ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved m-8ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved mls series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved mm series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved mms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved ms series</td>
<td></td>
</tr>
<tr>
<td>UK West 1 Year Reserved mts series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved a series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved am series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved d series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved ds series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved e series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved e-2s series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved e-32s series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved e-4s series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved e-8s series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved el series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved els series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved es series</td>
<td></td>
</tr>
<tr>
<td>UK West 3 Year Reserved f series</td>
<td></td>
</tr>
</tbody>
</table>
UK West 3 Year Reserved f1 series
UK West 3 Year Reserved f4 series
UK West 3 Year Reserved fs series
UK West 3 Year Reserved m series
UK West 3 Year Reserved m-16ms series
UK West 3 Year Reserved m-32ms series
UK West 3 Year Reserved m-64ms series
UK West 3 Year Reserved m-8ms series
UK West 3 Year Reserved mls series
UK West 3 Year Reserved mm series
UK West 3 Year Reserved mms series
UK West 3 Year Reserved ms series
UK West 3 Year Reserved mts series
US Gov Arizona d series
US Gov Arizona ds series
US Gov Arizona ei series
US Gov Arizona eis series
US Gov Arizona es series
US Gov Arizona g series
US Gov Arizona gs series
US Gov Arizona hc44rs series
US Gov Arizona ls series
US Gov Arizona m-8ms series
US Gov Arizona mms series
US Gov Arizona ms series
US Gov Arizona ms series
US Gov Arizona 1 Year Reserved a series
US Gov Arizona 1 Year Reserved am series
US Gov Arizona 1 Year Reserved d series
US Gov Arizona 1 Year Reserved ds series
US Gov Arizona 1 Year Reserved e series
US Gov Arizona 1 Year Reserved e-2s series
US Gov Arizona 1 Year Reserved e-32s series
US Gov Arizona 1 Year Reserved e-4s series
US Gov Arizona 1 Year Reserved e-8s series
US Gov Arizona 1 Year Reserved ei series
US Gov Arizona 1 Year Reserved es series
US Gov Arizona 1 Year Reserved f series
US Gov Arizona 1 Year Reserved f1 series
US Gov Arizona 1 Year Reserved f4 series
US Gov Arizona 1 Year Reserved fs series
US Gov Arizona 1 Year Reserved g series
US Gov Arizona 1 Year Reserved gs series
US Gov Arizona 1 Year Reserved h series
US Gov Arizona 1 Year Reserved hc44rs series
US Gov Arizona 1 Year Reserved ls series
US Gov Arizona 1 Year Reserved m series
US Gov Arizona 1 Year Reserved m-16ms series
US Gov Arizona 1 Year Reserved m-32ms series
US Gov Arizona 1 Year Reserved m-64ms series
US Gov Arizona 1 Year Reserved m-8ms series
US Gov Arizona 1 Year Reserved mls series
US Gov Arizona 1 Year Reserved mm series
US Gov Arizona 1 Year Reserved mms series
US Gov Arizona 1 Year Reserved ms series
US Gov Arizona 1 Year Reserved mts series
US Gov Arizona 3 Year Reserved a series
US Gov Arizona 3 Year Reserved am series
US Gov Arizona 3 Year Reserved d series
US Gov Arizona 3 Year Reserved ds series
US Gov Arizona 3 Year Reserved e series
US Gov Arizona 3 Year Reserved e-2s series
US Gov Arizona 3 Year Reserved e-32s series
US Gov Arizona 3 Year Reserved e-4s series
US Gov Arizona 3 Year Reserved e-8s series
US Gov Arizona 3 Year Reserved ei series
US Gov Arizona 3 Year Reserved eis series
US Gov Arizona 3 Year Reserved es series
US Gov Arizona 3 Year Reserved f series
US Gov Arizona 3 Year Reserved f1 series
US Gov Arizona 3 Year Reserved f4 series
US Gov Arizona 3 Year Reserved fs series
US Gov Arizona 3 Year Reserved g series
US Gov Arizona 3 Year Reserved gs series
US Gov Arizona 3 Year Reserved h series
US Gov Arizona 3 Year Reserved hc44rs series
US Gov Arizona 3 Year Reserved ls series
US Gov Arizona 3 Year Reserved m series
US Gov Arizona 3 Year Reserved m-16ms series
US Gov Arizona 3 Year Reserved m-32ms series
US Gov Arizona 3 Year Reserved m-64ms series
US Gov Arizona 3 Year Reserved m-8ms series
US Gov Arizona 3 Year Reserved mls series
US Gov Arizona 3 Year Reserved mm series
US Gov Arizona 3 Year Reserved mms series
US Gov Arizona 3 Year Reserved ms series
US Gov Arizona 3 Year Reserved mts series
US Gov Iowa d series
US Gov Iowa ds series
US Gov Iowa e series
US Gov Iowa e-2s series
US Gov Iowa e-32s series
US Gov Iowa e-4s series
US Gov Iowa e-8s series
US Gov Iowa es series
US Gov Iowa f series
US Gov Iowa fs series
US Gov Iowa g series
US Gov Iowa gs series
US Gov Iowa ls series
US Gov Iowa m series
US Gov Iowa m-16ms series
US Gov Iowa m-32ms series
US Gov Iowa m-64ms series
US Gov Iowa m-8ms series
US Gov Iowa mls series
US Gov Iowa mm series
US Gov Iowa mms series
US Gov Iowa ms series
US Gov Iowa mts series
US Gov Iowa 1 Year Reserved a series
US Gov Iowa 1 Year Reserved am series
US Gov Iowa 1 Year Reserved d series
US Gov Iowa 1 Year Reserved ds series
US Gov Iowa 1 Year Reserved e series
US Gov Iowa 1 Year Reserved e-2s series
US Gov Iowa 1 Year Reserved e-32s series
US Gov Iowa 1 Year Reserved e-4s series
US Gov Iowa 1 Year Reserved e-8s series
US Gov Iowa 1 Year Reserved es series
US Gov Iowa 1 Year Reserved f series
US Gov Iowa 1 Year Reserved f1 series
US Gov Iowa 1 Year Reserved f4 series
US Gov Iowa 1 Year Reserved fs series
US Gov Iowa 1 Year Reserved g series
US Gov Iowa 1 Year Reserved gs series
US Gov Iowa 1 Year Reserved ls series
US Gov Iowa 1 Year Reserved m series
US Gov Iowa 1 Year Reserved m-16ms series
US Gov Iowa 1 Year Reserved m-32ms series
US Gov Iowa 1 Year Reserved m-64ms series
US Gov Iowa 1 Year Reserved m-8ms series
US Gov Iowa 1 Year Reserved mls series
US Gov Iowa 1 Year Reserved mm series
US Gov Iowa 1 Year Reserved mms series
US Gov Iowa 1 Year Reserved ms series
US Gov Iowa 1 Year Reserved mts series
US Gov Iowa 3 Year Reserved a series
US Gov Iowa 3 Year Reserved am series
US Gov Iowa 3 Year Reserved d series
US Gov Iowa 3 Year Reserved e series
US Gov Iowa 3 Year Reserved e-2s series
US Gov Iowa 3 Year Reserved e-32s series
US Gov Iowa 3 Year Reserved e-4s series
US Gov Iowa 3 Year Reserved e-8s series
US Gov Iowa 3 Year Reserved es series
US Gov Iowa 3 Year Reserved f series
US Gov Iowa 3 Year Reserved f1 series
US Gov Iowa 3 Year Reserved f4 series
US Gov Iowa 3 Year Reserved fs series
US Gov Iowa 3 Year Reserved g series
US Gov Iowa 3 Year Reserved gs series
US Gov Iowa 3 Year Reserved ls series
US Gov Iowa 3 Year Reserved m series
US Gov Iowa 3 Year Reserved m-16ms series
US Gov Iowa 3 Year Reserved m-32ms series
US Gov Iowa 3 Year Reserved m-64ms series
US Gov Iowa 3 Year Reserved m-8ms series
US Gov Iowa 3 Year Reserved mls series
US Gov Iowa 3 Year Reserved mm series
US Gov Iowa 3 Year Reserved mms series
US Gov Iowa 3 Year Reserved ms series
US Gov Iowa 3 Year Reserved mts series
US Gov Texas d series
US Gov Texas ds series
US Gov Texas es series
US Gov Texas f series
US Gov Texas fs series
US Gov Texas g series
US Gov Texas gs series
US Gov Texas ls series
US Gov Texas 1 Year Reserved a series
US Gov Texas 1 Year Reserved am series
US Gov Texas 1 Year Reserved d series
US Gov Texas 1 Year Reserved ds series
US Gov Texas 1 Year Reserved e series
US Gov Texas 1 Year Reserved e-2s series
US Gov Texas 1 Year Reserved e-32s series
US Gov Texas 1 Year Reserved e-4s series
US Gov Texas 1 Year Reserved e-8s series
US Gov Texas 1 Year Reserved es series
US Gov Texas 1 Year Reserved f series
US Gov Texas 1 Year Reserved f1 series
US Gov Texas 1 Year Reserved f4 series
US Gov Texas 1 Year Reserved fs series
US Gov Texas 1 Year Reserved g series
US Gov Texas 1 Year Reserved gs series
US Gov Texas 1 Year Reserved ls series
US Gov Texas 3 Year Reserved a series
US Gov Texas 3 Year Reserved am series
US Gov Texas 3 Year Reserved d series
US Gov Texas 3 Year Reserved ds series
US Gov Texas 3 Year Reserved e series
US Gov Texas 3 Year Reserved e-2s series
US Gov Texas 3 Year Reserved e-32s series
US Gov Texas 3 Year Reserved e-4s series
US Gov Texas 3 Year Reserved e-8s series
US Gov Texas 3 Year Reserved es series
US Gov Texas 3 Year Reserved f series
US Gov Texas 3 Year Reserved f1 series
US Gov Texas 3 Year Reserved f4 series
US Gov Texas 3 Year Reserved fs series
US Gov Texas 3 Year Reserved g series
US Gov Texas 3 Year Reserved gs series
US Gov Texas 3 Year Reserved ls series
US Gov Virginia d series
US Gov Virginia ds series
US Gov Virginia e series
US Gov Virginia ei series
US Gov Virginia eis series
US Gov Virginia es series
US Gov Virginia fs series
US Gov Virginia hc44rs series
US Gov Virginia ls series
US Gov Virginia m-8ms series
US Gov Virginia mms series
US Gov Virginia ms series
US Gov Virginia 1 Year Reserved a series
US Gov Virginia 1 Year Reserved am series
US Gov Virginia 1 Year Reserved d series
US Gov Virginia 1 Year Reserved ds series
US Gov Virginia 1 Year Reserved e series
US Gov Virginia 1 Year Reserved e-2s series
US Gov Virginia 1 Year Reserved e-32s series
US Gov Virginia 1 Year Reserved e-4s series
US Gov Virginia 1 Year Reserved e-8s series
US Gov Virginia 1 Year Reserved ei series
US Gov Virginia 1 Year Reserved eis series
US Gov Virginia 1 Year Reserved es series
US Gov Virginia 1 Year Reserved f series
US Gov Virginia 1 Year Reserved f1 series
US Gov Virginia 1 Year Reserved f4 series
US Gov Virginia 1 Year Reserved fs series
US Gov Virginia 1 Year Reserved g series
US Gov Virginia 1 Year Reserved gs series
US Gov Virginia 1 Year Reserved hc44rs series
US Gov Virginia 1 Year Reserved ls series
US Gov Virginia 1 Year Reserved m series
US Gov Virginia 1 Year Reserved m-16ms series
US Gov Virginia 1 Year Reserved m-32ms series
US Gov Virginia 1 Year Reserved m-64ms series
US Gov Virginia 1 Year Reserved m-8ms series
US Gov Virginia 1 Year Reserved mls series
US Gov Virginia 1 Year Reserved mm series
US Gov Virginia 1 Year Reserved mms series
US Gov Virginia 1 Year Reserved ms series
US Gov Virginia 1 Year Reserved mts series
US Gov Virginia 3 Year Reserved a series
US Gov Virginia 3 Year Reserved am series
US Gov Virginia 3 Year Reserved d series
US Gov Virginia 3 Year Reserved ds series
US Gov Virginia 3 Year Reserved e series
US Gov Virginia 3 Year Reserved e-2s series
US Gov Virginia 3 Year Reserved e-32s series
US Gov Virginia 3 Year Reserved e-4s series
US Gov Virginia 3 Year Reserved e-8s series
US Gov Virginia 3 Year Reserved ei series
US Gov Virginia 3 Year Reserved eis series
US Gov Virginia 3 Year Reserved es series
US Gov Virginia 3 Year Reserved f series
US Gov Virginia 3 Year Reserved f1 series
US Gov Virginia 3 Year Reserved f4 series
US Gov Virginia 3 Year Reserved fs series
US Gov Virginia 3 Year Reserved g series
US Gov Virginia 3 Year Reserved gs series
US Gov Virginia 3 Year Reserved hs series
US Gov Virginia 3 Year Reserved ls series
US Gov Virginia 3 Year Reserved m series
US Gov Virginia 3 Year Reserved m-16ms series
US Gov Virginia 3 Year Reserved m-32ms series
US Gov Virginia 3 Year Reserved m-64ms series
US Gov Virginia 3 Year Reserved m-8ms series
US Gov Virginia 3 Year Reserved mls series
US Gov Virginia 3 Year Reserved mm series
US Gov Virginia 3 Year Reserved mms series
US Gov Virginia 3 Year Reserved ms series
US Gov Virginia 3 Year Reserved mts series
West Central US d series
West Central US ds series
West Central US e series
West Central US e-2s series
West Central US e-32s series
West Central US e-4s series
West Central US e-8s series
West Central US ei series
West Central US eis series
West Central US es series
West Central US f series
West Central US fs series
West Central US 1 Year Reserved a series
West Central US 1 Year Reserved am series
West Central US 1 Year Reserved d series
West Central US 1 Year Reserved ds series
West Central US 1 Year Reserved e series
West Central US 1 Year Reserved e-2s series
West Central US 1 Year Reserved e-32s series
West Central US 1 Year Reserved e-4s series
West Central US 1 Year Reserved e-8s series
West Central US 1 Year Reserved ei series
West Central US 1 Year Reserved eis series
West Central US 1 Year Reserved es series
West Central US 1 Year Reserved f series
West Central US 1 Year Reserved f1 series
West Central US 1 Year Reserved f4 series
West Central US 3 Year Reserved a series
West Central US 3 Year Reserved am series
West Central US 3 Year Reserved d series
West Central US 3 Year Reserved ds series
West Central US 3 Year Reserved e series
West Central US 3 Year Reserved e-2s series
West Central US 3 Year Reserved e-32s series
West Central US 3 Year Reserved e-4s series
West Central US 3 Year Reserved e-8s series
West Central US 3 Year Reserved ei series
West Central US 3 Year Reserved eis series
West Central US 3 Year Reserved es series
West Central US 3 Year Reserved f series
West Central US 3 Year Reserved f1 series
West Central US 3 Year Reserved f4 series
West Central US 3 Year Reserved fs series
West Europe d series
West Europe da series
West Europe das series
West Europe ds series
West Europe ea series
West Europe eas series
West Europe ls series
West Europe m-8ms series
West Europe mms series
West Europe ms series
West Europe 1 Year Reserved a series
West Europe 1 Year Reserved am series
West Europe 1 Year Reserved d series
West Europe 1 Year Reserved da series
West Europe 1 Year Reserved das series
West Europe 1 Year Reserved dc2s series
West Europe 1 Year Reserved dc4s series
West Europe 1 Year Reserved ds series
West Europe 1 Year Reserved e series
West Europe 1 Year Reserved e-2s series
West Europe 1 Year Reserved e-32s series
West Europe 1 Year Reserved e-4s series
West Europe 1 Year Reserved e-8s series
West Europe 1 Year Reserved ea series
West Europe 1 Year Reserved eas series
West Europe 1 Year Reserved ei series
West Europe 1 Year Reserved eis series
West Europe 1 Year Reserved es series
West Europe 1 Year Reserved f series
West Europe 1 Year Reserved f1 series
West Europe 1 Year Reserved f4 series
West Europe 1 Year Reserved fs series
West Europe 1 Year Reserved g series
West Europe 1 Year Reserved gs series
West Europe 1 Year Reserved h series
West Europe 1 Year Reserved hc44rs series
West Europe 1 Year Reserved l series
West Europe 1 Year Reserved ls series
West Europe 1 Year Reserved m series
West Europe 1 Year Reserved m-16ms series
West Europe 1 Year Reserved m-32ms series
West Europe 1 Year Reserved m-64ms series
West Europe 1 Year Reserved m-8ms series
West Europe 1 Year Reserved mls series
West Europe 1 Year Reserved mm series
West Europe 1 Year Reserved mms series
West Europe 1 Year Reserved ms series
West Europe 1 Year Reserved mts series
West Europe 3 Year Reserved a series
West Europe 3 Year Reserved am series
West Europe 3 Year Reserved d series
West Europe 3 Year Reserved da series
West Europe 3 Year Reserved das series
West Europe 3 Year Reserved dc2s series
West Europe 3 Year Reserved dc4s series
West Europe 3 Year Reserved ds series
West Europe 3 Year Reserved e series
West Europe 3 Year Reserved e-2s series
West Europe 3 Year Reserved e-32s series
West Europe 3 Year Reserved e-4s series
West Europe 3 Year Reserved e-8s series
West Europe 3 Year Reserved ea series
West Europe 3 Year Reserved eas series
West Europe 3 Year Reserved ei series
West Europe 3 Year Reserved eis series
West Europe 3 Year Reserved es series
West Europe 3 Year Reserved f series
West Europe 3 Year Reserved f1 series
West Europe 3 Year Reserved f4 series
West Europe 3 Year Reserved fs series
West Europe 3 Year Reserved g series
West Europe 3 Year Reserved gs series
West Europe 3 Year Reserved h series
West Europe 3 Year Reserved hc44rs series
West Europe 3 Year Reserved l series
West Europe 3 Year Reserved ls series
West Europe 3 Year Reserved m series
West Europe 3 Year Reserved m-16ms series
West Europe 3 Year Reserved m-32ms series
West Europe 3 Year Reserved m-64ms series
West Europe 3 Year Reserved m-8ms series
West Europe 3 Year Reserved mls series
West Europe 3 Year Reserved mm series
West Europe 3 Year Reserved mms series
West Europe 3 Year Reserved ms series
West Europe 3 Year Reserved mts series
West India d series
West India ds series
West India e series
West India e-2s series
West India e-32s series
West India e-4s series
West India e-8s series
West India es series
West India 1 Year Reserved a series
West India 1 Year Reserved am series
West India 1 Year Reserved d series
West India 1 Year Reserved ds series
West India 1 Year Reserved e series
West India 1 Year Reserved e-2s series
West India 1 Year Reserved e-32s series
West India 1 Year Reserved e-4s series
West India 1 Year Reserved e-8s series
West India 1 Year Reserved el series
West India 1 Year Reserved els series
West India 1 Year Reserved es series
West India 1 Year Reserved f series
West India 1 Year Reserved f1 series
West India 1 Year Reserved f4 series
West India 1 Year Reserved fs series
West India 3 Year Reserved a series
West India 3 Year Reserved am series
West India 3 Year Reserved d series
West India 3 Year Reserved ds series
West India 3 Year Reserved e series
West India 3 Year Reserved e-2s series
West India 3 Year Reserved e-32s series
West India 3 Year Reserved e-4s series
West India 3 Year Reserved e-8s series
West India 3 Year Reserved el series
West India 3 Year Reserved els series
West India 3 Year Reserved es series
West India 3 Year Reserved f series
West India 3 Year Reserved f1 series
West India 3 Year Reserved f4 series
West India 3 Year Reserved fs series
West India 3 Year Reserved mls series
West India 3 Year Reserved mm series
West India 3 Year Reserved mms series
West India 3 Year Reserved ms series
West India 3 Year Reserved mts series
West US d series
West US ds series
West US 1 series
West US ls series
West US 1 Year Reserved a series
West US 1 Year Reserved am series
West US 1 Year Reserved d series
West US 1 Year Reserved ds series
West US 1 Year Reserved e series
West US 1 Year Reserved e-2s series
West US 1 Year Reserved e-32s series
West US 1 Year Reserved e-4s series
West US 1 Year Reserved e-8s series
West US 1 Year Reserved el series
West US 1 Year Reserved eis series
West US 1 Year Reserved es series
West US 1 Year Reserved f series
West US 1 Year Reserved f1 series
West US 1 Year Reserved f4 series
West US 1 Year Reserved fs series
West US 1 Year Reserved g series
West US 1 Year Reserved gs series
West US 1 Year Reserved h series
West US 1 Year Reserved l series
West US 1 Year Reserved ls series
West US 2 d series
West US 2 da series
West US 2 das series
West US 2 ds series
West US 2 ea series
West US 2 eas series
West US 2 f series
West US 2 fs series
West US 2 g series
West US 2 gs series
West US 2 ls series
West US 2 m-16ms series
West US 2 m-32ms series
West US 2 m-8ms series
West US 2 mm series
West US 2 mms series
West US 2 ms series
West US 2 1 Year Reserved a series
West US 2 1 Year Reserved am series
West US 2 1 Year Reserved d series
West US 2 1 Year Reserved da series
West US 2 1 Year Reserved das series
West US 2 1 Year Reserved ds series
West US 2 1 Year Reserved e series
West US 2 1 Year Reserved e-2s series
West US 2 1 Year Reserved e-32s series
West US 2 1 Year Reserved e-4s series
West US 2 1 Year Reserved e-8s series
West US 2 1 Year Reserved ea series
West US 2 1 Year Reserved eas series
West US 2 1 Year Reserved el series
West US 2 1 Year Reserved eis series
West US 2 1 Year Reserved es series
West US 2 1 Year Reserved f series
West US 2 1 Year Reserved f1 series
West US 2 1 Year Reserved f4 series
West US 2 1 Year Reserved fs series
West US 2 1 Year Reserved g series
West US 2 1 Year Reserved gs series
West US 2 1 Year Reserved h series
West US 2 1 Year Reserved l series
West US 2 1 Year Reserved ls series
West US 2 1 Year Reserved es series
West US 2 1 Year Reserved f series
West US 2 1 Year Reserved f1 series
West US 2 1 Year Reserved f4 series
West US 2 1 Year Reserved fs series
West US 2 1 Year Reserved g series
West US 2 1 Year Reserved gs series
West US 2 1 Year Reserved h series
West US 2 1 Year Reserved hc44rs series
West US 2 1 Year Reserved l series
West US 2 1 Year Reserved ls series
West US 2 1 Year Reserved m series
West US 2 1 Year Reserved m-16ms series
West US 2 1 Year Reserved m-32ms series
West US 2 1 Year Reserved m-64ms series
West US 2 1 Year Reserved m-8ms series
West US 2 1 Year Reserved mls series
West US 2 1 Year Reserved mm series
West US 2 1 Year Reserved mms series
West US 2 1 Year Reserved ms series
West US 2 1 Year Reserved mts series
West US 2 3 Year Reserved a series
West US 2 3 Year Reserved am series
West US 2 3 Year Reserved d series
West US 2 3 Year Reserved da series
West US 2 3 Year Reserved das series
West US 2 3 Year Reserved ds series
West US 2 3 Year Reserved e series
West US 2 3 Year Reserved e-2s series
West US 2 3 Year Reserved e-32s series
West US 2 3 Year Reserved e-4s series
West US 2 3 Year Reserved e-8s series
West US 2 3 Year Reserved ea series
West US 2 3 Year Reserved eas series
West US 2 3 Year Reserved ei series
West US 2 3 Year Reserved eis series
West US 2 3 Year Reserved es series
West US 2 3 Year Reserved f series
West US 2 3 Year Reserved f1 series
West US 2 3 Year Reserved f4 series
West US 2 3 Year Reserved fs series
West US 2 3 Year Reserved g series
West US 2 3 Year Reserved gs series
West US 2 3 Year Reserved h series
West US 2 3 Year Reserved hc44rs series
West US 2 3 Year Reserved l series
West US 2 3 Year Reserved ls series
West US 2 3 Year Reserved m series
West US 2 3 Year Reserved m-16ms series
West US 2 3 Year Reserved m-32ms series
West US 2 3 Year Reserved m-64ms series
West US 2 3 Year Reserved m-8ms series
West US 2 3 Year Reserved mls series
West US 2 3 Year Reserved mm series
West US 2 3 Year Reserved mms series
West US 2 3 Year Reserved ms series
West US 3 Year Reserved mts series
West US 3 Year Reserved am series
West US 3 Year Reserved d series
West US 3 Year Reserved ds series
West US 3 Year Reserved e series
West US 3 Year Reserved e-2s series
West US 3 Year Reserved e-32s series
West US 3 Year Reserved e-4s series
West US 3 Year Reserved e-8s series
West US 3 Year Reserved e1 series
West US 3 Year Reserved els series
West US 3 Year Reserved es series
West US 3 Year Reserved f series
West US 3 Year Reserved f1 series
West US 3 Year Reserved f4 series
West US 3 Year Reserved fs series
West US 3 Year Reserved g series
West US 3 Year Reserved gs series
West US 3 Year Reserved h series
West US 3 Year Reserved l series
West US 3 Year Reserved ls series

Agilisys Updates / August 22, 2019

2GB → 64GB Windows + Linux VMs
(CURRENT GBP TO USD CONVERSION = 1.22)

AWS Updates / March 4, 2019

- New Locations
- New Instances

New Locations

EU (Stockholm)
AWS GovCloud (US-East)

New Instances

Asia Mumbai c5d series
Asia Mumbai m5 series
Asia Mumbai m5d series
Asia Mumbai r5 series
Asia Mumbai r5d series
Asia Seoul m5 series
Asia Seoul m5d series
Asia Seoul r5 series
Asia Seoul r5d series
Asia Seoul x1e series
Asia Singapore m5 series
Asia Singapore m5d series
Asia Singapore r5 series
Asia Singapore r5d series
Asia Singapore z1d series
Asia Tokyo i3 series
Asia Tokyo m5 series
Asia Tokyo r5 series
Asia Tokyo r5d series
Asia Tokyo z1d series
Canada Central r5 series
Canada Central r5d series
EU Frankfurt i3 series
EU Frankfurt m5 series
EU Frankfurt m5d series
EU Frankfurt r5 series
EU Frankfurt r5d series
EU Ireland i3 series
EU Ireland m5 series
EU Ireland m5d series
EU Ireland r5 series
EU Ireland r5d series
EU Ireland z1d series
EU London m5 series
EU London r5 series
EU London r5d series
EU Paris m5 series
EU Paris m5d series
EU Paris r5 series
EU Paris r5d series
GovCloud i3 series
GovCloud r5 series
GovCloud r5d series
Pacific Sydney m5 series
Pacific Sydney m5d series
Pacific Sydney r5 series
Pacific Sydney r5d series
US California i3 series
US California m5 series
US California r5 series
US California r5d series
US California z1d series
US Ohio i3 series
US Ohio m5 series
US Ohio m5d series
US Ohio r5 series
US Ohio r5d series
US Oregon i3 series
US Oregon m5 series
US Oregon m5d series
US Oregon r5 series
US Oregon r5d series
US Oregon z1d series
US Virginia i3 series
US Virginia m5 series
US Virginia m5d series
US Virginia r5 series
US Virginia r5d series
US Virginia z1d series
Updated Instances:
Asia Mumbai x1.16xlarge
Asia Mumbai x1.32xlarge

**Azure Updates / March 4, 2019**

**New Instances**
- Australia Central e64-16s-v3
- Australia Central e64-32s-v3
- Australia Central e64-v3
- Australia Central e64s-v3
- Australia Central e8-4s-v3
- Australia Central f16s-v2
- Australia Central f2s-v2
- Australia Central f32s-v2
- Australia Central f4s-v2
- Australia Central f4s-v3
- Australia Central f64s-v2
- Australia Central f72s-v2
- Australia Central f8s-v2
- Australia Central m128
- Australia Central m128-32ms
- Australia Central m128-64ms
- Australia Central m128m
- Australia Central m128ms
- Australia Central m128s
- Australia Central m16ms
- Australia Central m32ls
- Australia Central m32ms
- Australia Central m32ts
- Australia Central m64
- Australia Central m64-16ms
- Australia Central m64-32ms
- Australia Central m64ls
- Australia Central m64ms
- Australia Central m64s
- Australia Central m8ms
- Australia Central 2 e64-16s-v3
- Australia Central 2 e64-32s-v3
- Australia Central 2 e64-v3
- Australia Central 2 e64s-v3
- Australia Central 2 e8-4s-v3
- Australia Central 2 f16s-v2
- Australia Central 2 f2s-v2
- Australia Central 2 f32s-v2
- Australia Central 2 f4s-v2
- Australia Central 2 f4s-v3
- Australia Central 2 f72s-v2
- Australia Central 2 f8s-v2
- Australia Central 2 m128
- Australia Central 2 m128m
- Australia Central 2 m128ms
- Australia Central 2 m128s
- Australia Central 2 m16ms
- Australia Central 2 m32ls
- Australia Central 2 m32ms
- Australia Central 2 m32ts
Australia Central 2 m64
Australia Central 2 m64ls
Australia Central 2 m64m
Australia Central 2 m64ms
Australia Central 2 m64s
Australia Central 2 m8ms
Australia East e64-16s-v3
Australia East e64-32s-v3
Australia East e64-v3
Australia East e64i-v3
Australia East e64ls-v3
Australia East e64s-v3
Australia East e8-4s-v3
Australia Southeast e64-16s-v3
Australia Southeast e64-32s-v3
Australia Southeast e64-v3
Australia Southeast e64i-v3
Australia Southeast e64ls-v3
Australia Southeast e64s-v3
Australia Southeast e8-4s-v3
Australia Southeast f16s-v2
Australia Southeast f2s-v2
Australia Southeast f32s-v2
Australia Southeast f4s-v2
Australia Southeast f64s-v2
Australia Southeast f72s-v2
Australia Southeast f8s-v2
Brazil South e64-16s-v3
Brazil South e64-32s-v3
Brazil South e64-v3
Brazil South e64i-v3
Brazil South e64ls-v3
Brazil South e64s-v3
Brazil South e8-4s-v3
Canada Central e64-16s-v3
Canada Central e64-32s-v3
Canada Central e64-v3
Canada Central e64i-v3
Canada Central e64ls-v3
Canada Central e64s-v3
Canada Central e8-4s-v3
Canada East e64-16s-v3
Canada East e64-32s-v3
Canada East e64-v3
Canada East e64i-v3
Canada East e64ls-v3
Canada East e64s-v3
Canada East e8-4s-v3
Canada East f16s-v2
Canada East f2s-v2
Canada East f32s-v2
Canada East f4s-v2
Canada East f64s-v2
Canada East f72s-v2
Canada East f8s-v2
Central India e64-16s-v3
Central India e64-32s-v3
Central India e64-v3
Central India e64s-v3
Central India e8-4s-v3
Central US e64-16s-v3
Central US e64-32s-v3
Central US e64-v3
Central US e64i-v3
Central US e64is-v3
Central US e64s-v3
Central US e8-4s-v3
Central US f16s-v2
Central US f2s-v2
Central US f32s-v2
Central US f4s-v2
Central US f64s-v2
Central US f72s-v2
Central US f8s-v2
East Asia e64-16s-v3
East Asia e64-32s-v3
East Asia e64-v3
East Asia e64i-v3
East Asia e64is-v3
East Asia e64s-v3
East Asia e8-4s-v3
East Asia f16s-v2
East Asia f2s-v2
East Asia f32s-v2
East Asia f4s-v2
East Asia f64s-v2
East Asia f72s-v2
East Asia f8s-v2
East US e16-4s-v3
East US e16-8s-v3
East US e16-v3
East US e16s-v3
East US e2-v3
East US e20-v3
East US e20s-v3
East US e2s-v3
East US e32-16s-v3
East US e32-8s-v3
East US e32-v3
East US e32s-v3
East US e4-2s-v3
East US e4-v3
East US e4s-v3
East US e64-16s-v3
East US e64-32s-v3
East US e64-v3
East US e64i-v3
East US e64is-v3
East US e64s-v3
East US e8-2s-v3
East US e8-4s-v3
East US e8-v3
East US e8s-v3
East US l16s-v2
East US l32s-v2
East US l64s-v2
East US l8s-v2
East US 2 e64-16s-v3
East US 2 e64-32s-v3
East US 2 e64-v3
East US 2 e641-v3
East US 2 e641s-v3
East US 2 e64s-v3
East US 2 e8-4s-v3
East US 2 l16s-v2
East US 2 l32s-v2
East US 2 l64s-v2
East US 2 l8s-v2
France Central e64-v3
France Central e641-v3
France Central e641s-v3
France South e64-v3
France South e641-v3
France South e641s-v3
France South f16s-v2
France South f2s-v2
France South f32s-v2
France South f4s-v2
France South f64s-v3
France South f72s-v3
France South f8s-v2
Germany Central e8-4s-v3
Germany Northeast e8-4s-v3
Japan East e64-16s-v3
Japan East e64-32s-v3
Japan East e64-v3
Japan East e641-v3
Japan East e641s-v3
Japan East e64s-v3
Japan East e8-4s-v3
Japan West e64-16s-v3
Japan West e64-32s-v3
Japan West e64-v3
Japan West e641-v3
Japan West e641s-v3
Japan West e64s-v3
Japan West e8-4s-v3
Japan West f16s-v2
Japan West f2s-v2
Japan West f32s-v2
Japan West f4s-v2
Japan West f64s-v2
Japan West f72s-v2
Japan West f8s-v2
Korea Central e64-16s-v3
Korea Central e64-32s-v3
Korea Central e64-v3
Korea Central e641-v3
North Central US e8-2s-v3
North Central US e8-4s-v3
North Central US e8-v3
North Central US e8s-v3
North Europe e16-4s-v3
North Europe e16-8s-v3
North Europe e16-v3
North Europe e16s-v3
North Europe e2-v3
North Europe e20-v3
North Europe e20s-v3
North Europe e2s-v3
North Europe e32-16s-v3
North Europe e32-8s-v3
North Europe e32-v3
North Europe e32s-v3
North Europe e4-2s-v3
North Europe e4-v3
North Europe e4s-v3
North Europe e64-16s-v3
North Europe e64-32s-v3
North Europe e64-v3
North Europe e641-v3
North Europe e64is-v3
North Europe e64s-v3
North Europe e8-2s-v3
North Europe e8-4s-v3
North Europe e8-8s-v3
North Europe e8-v3
North Europe e8s-v3
South Central US e64-16s-v3
South Central US e64-32s-v3
South Central US e64-v3
South Central US e641-v3
South Central US e64is-v3
South Central US e64s-v3
South Central US e8-4s-v3
South Central US f16s-v2
South Central US f2s-v2
South Central US f32s-v2
South Central US f4s-v2
South Central US f64s-v2
South Central US f72s-v2
South Central US f8s-v2
South India e64-16s-v3
South India e64-32s-v3
South India e64-v3
South India e641-v3
South India e64is-v3
South India e64s-v3
South India e8-4s-v3
South India f16s-v2
South India f2s-v2
South India f32s-v2
South India f4s-v2
South India f64s-v2
South India f72s-v2
South India f8s-v2
Southeast Asia e64-16s-v3
Southeast Asia e64-32s-v3
Southeast Asia e64-v3
Southeast Asia e641-v3
Southeast Asia e64is-v3
Southeast Asia e64s-v3
Southeast Asia e8-4s-v3
Southeast Asia l16s-v2
Southeast Asia l32s-v2
Southeast Asia l64s-v2
Southeast Asia l8s-v2
UK South e64-16s-v3
UK South e64-32s-v3
UK South e64-v3
UK South e641-v3
UK South e64is-v3
UK South e64s-v3
UK South e8-4s-v3
UK West e64-16s-v3
UK West e64-32s-v3
UK West e64-v3
UK West e641-v3
UK West e64is-v3
UK West e64s-v3
UK West e8-4s-v3
US Gov Arizona e64-16s-v3
US Gov Arizona e64-32s-v3
US Gov Arizona e64-v3
US Gov Arizona e64s-v3
US Gov Arizona e8-4s-v3
US Gov Texas e64-16s-v3
US Gov Texas e64-32s-v3
US Gov Texas e64-v3
US Gov Texas e64s-v3
US Gov Texas e8-4s-v3
US Gov Virginia d16-v3
US Gov Virginia d16s-v3
US Gov Virginia d2-v3
US Gov Virginia d2s-v3
US Gov Virginia d32-v3
US Gov Virginia d4s-v3
US Gov Virginia d64-v3
US Gov Virginia d64s-v3
US Gov Virginia d8-v3
US Gov Virginia d8s-v3
US Gov Virginia e16-4s-v3
US Gov Virginia e16-8s-v3
US Gov Virginia e16-v3
US Gov Virginia e16s-v3
US Gov Virginia e2-v3
US Gov Virginia e20-v3
US Gov Virginia e20s-v3
US Gov Virginia e2s-v3
Chapter 4  Using the Platform

Reports/Pages

AWS Updates / January 3, 2019

New Instances

Asia Mumbai c5 series
Asia Mumbai i3 series
Asia Mumbai m4 series
Asia Mumbai x1 series
Asia Seoul c5 series
Asia Seoul c5d series
Asia Seoul i3 series
Asia Seoul m4 series
Asia Seoul m5d series
Asia Seoul r5 series
Asia Seoul r5d series
Asia Seoul x1 series
Asia Singapore c5 series
Asia Singapore c5d series
Asia Singapore i3 series
Asia Singapore m4 series
Asia Singapore m5d series
Asia Singapore r5 series
Asia Singapore r5a series
Asia Singapore r5d series
Asia Singapore x1 series
Asia Singapore z1d series
Asia Tokyo c5 series
Asia Tokyo c5d series
Asia Tokyo i3 series
Asia Tokyo m4 series
Asia Tokyo m5d series
Asia Tokyo r5 series
Asia Tokyo r5d series
Asia Tokyo x1 series
Asia Tokyo x1e series
Asia Tokyo z1d series
Canada Central c5 series
Canada Central c5d series
Canada Central i3 series
Canada Central m4 series
Canada Central m5d series
Canada Central r5 series
Canada Central r5d series
Canada Central x1 series
EU Frankfurt c5 series
EU Frankfurt c5d series
EU Frankfurt i3 series
EU Frankfurt m4 series
EU Frankfurt m5d series
EU Frankfurt r5 series
EU Frankfurt r5d series
EU Frankfurt x1 series
EU Frankfurt x1e series
EU Ireland a1 series
EU Ireland c5 series
EU Ireland c5d series
EU Ireland c5n series
EU Ireland h1 series
EU Ireland i3 series
EU Ireland m4 series
EU Ireland m5d series
EU Ireland r5 series
EU Ireland r5a series
EU Ireland r5d series
EU Ireland x1 series
EU Ireland x1e series
EU Ireland z1d series
EU London c5 series
EU London c5d series
EU London i3 series
EU London m4 series
EU London m5d series
EU London r5 series
EU London r5d series
EU London x1 series
EU Paris c5 series
EU Paris c5d series
EU Paris i3 series
EU Paris m5d series
EU Paris r5 series
EU Paris r5d series
EU Paris x1 series
GovCloud c5d series
GovCloud c5n series
GovCloud i3 series
GovCloud m4 series
GovCloud m5d series
GovCloud r5 series
GovCloud r5d series
GovCloud x1 series
GovCloud x1e series
Pacific Sydney c5 series
Pacific Sydney c5d series
Pacific Sydney i3 series
Pacific Sydney m4 series
Pacific Sydney m5d series
Pacific Sydney r5 series
Pacific Sydney r5d series
Pacific Sydney x1 series
Pacific Sydney x1e series
South America c5 series
South America i3 series
South America m4 series
South America x1 series
US California c5 series
US California c5d series
US California i3 series
US California m4 series
US California m5d series
US California r5 series
US California r5d series
US California z1d series
US Ohio a1 series
US Ohio c5 series
US Ohio c5d series
US Ohio c5n series
US Ohio h1 series
US Ohio i3 series
US Ohio m4 series
US Ohio m5d series
US Ohio r5 series
US Ohio r5a series
US Ohio r5d series
US Ohio x1 series
US Oregon a1 series
US Oregon c5 series
US Oregon c5d series
US Oregon c5n series
US Oregon h1 series
US Oregon i3 series
US Oregon m4 series
US Oregon m5d series
US Oregon r5 series
US Oregon r5a series
US Oregon r5d series
US Oregon x1 series
US Oregon x1e series
US Oregon z1d series
US Virginia a1 series
US Virginia c5 series
US Virginia c5d series
US Virginia c5n series
US Virginia h1 series
US Virginia i3 series
US Virginia m4 series
US Virginia m5d series
US Virginia r5 series
US Virginia r5a series
US Virginia r5d series
US Virginia x1 series
US Virginia x1e series
US Virginia z1d series
Azure Updates / January 3, 2019

East US 116s-v2 series
East US 132s-v2 series
East US 164s-v2 series
East US 180s-v2 series
East US 18s-v2 series
East US m128 series
East US m128-32ms series
East US m128-64ms series
East US m128m series
East US m128ms series
East US m128s series
East US m128s series
East US m16ms series
East US m32ls series
East US m32ms series
East US m32ts series
East US m64 series
East US m64-16ms series
East US m64-32ms series
East US m64ls series
East US m64m series
East US m64ms series
East US m64s series
East US m8ms series
East US 2 116s-v2 series
East US 2 132s-v2 series
East US 2 164s-v2 series
East US 2 180s-v2 series
East US 2 18s-v2 series
East US 2 m128 series
East US 2 m128-32ms series
East US 2 m128-64ms series
East US 2 m128m series
East US 2 m128ms series
East US 2 m128s series
East US 2 m16ms series
East US 2 m32ls series
East US 2 m32ms series
East US 2 m32ts series
East US 2 m64 series
East US 2 m64-16ms series
East US 2 m64-32ms series
East US 2 m64ls series
East US 2 m64m series
East US 2 m64ms series
East US 2 m64s series
East US 2 m8ms series
US Gov Virginia m128 series
US Gov Virginia m128-32ms series
US Gov Virginia m128-64ms series
US Gov Virginia m128m series
US Gov Virginia m128ms series
US Gov Virginia m128s series
US Gov Virginia m16ms series
US Gov Virginia m32ls series
US Gov Virginia m32ms series
Chapter 4 Using the Platform

Reports/Pages

US Gov Virginia m32ts series
US Gov Virginia m64 series
US Gov Virginia m64-16ms series
US Gov Virginia m64-32ms series
US Gov Virginia m64ls series
US Gov Virginia m64m series
US Gov Virginia m64ms series
US Gov Virginia m64s series
US Gov Virginia m8ms series
North Europe m128 series
North Europe m128-32ms series
North Europe m128-64ms series
North Europe m128m series
North Europe m128ms series
North Europe m128s series
North Europe m16ms series
North Europe m32ls series
North Europe m32ms series
North Europe m32ts series
North Europe m64 series
North Europe m64-16ms series
North Europe m64-32ms series
North Europe m64ls series
North Europe m64m series
North Europe m64ms series
North Europe m64s series
North Europe m8ms series
West Europe m116s-v2 series
West Europe m132s-v2 series
West Europe m164s-v2 series
West Europe m180s-v2 series
West Europe m18s-v2 series
West Europe m128 series
West Europe m128-32ms series
West Europe m128-64ms series
West Europe m128m series
West Europe m16ms series
West Europe m32ls series
West Europe m32ms series
West Europe m32ts series
West Europe m64 series
West Europe m64-16ms series
West Europe m64-32ms series
West Europe m64ls series
West Europe m64m series
West Europe m64ms series
West Europe m64s series
West Europe m8ms series
West Europe m64s series
West Europe m64ls series
West Europe m64ms series
West Europe m64s series
West Europe m64ms series
West Europe m64s series
West Europe m64ms series
West Europe m64s series
Australia East m128 series
Australia East m128-32ms series
Australia East m128-64ms series
Australia East m128ms series
Australia East m128s series
Australia East m128ms series
Australia East m128s series
Australia East m16ms series
Australia East m32ls series
Australia East m32ms series
Australia East m32ts series
Australia East m64 series
Australia East m64-16ms series
Australia East m64-32ms series
Australia East m64ls series
Australia East m64m series
Australia East m64ms series
Australia East m64s series
Australia East m8ms series
Australia Southeast m128 series
Australia Southeast m128-32ms series
Australia Southeast m128-64ms series
Australia Southeast m128m series
Australia Southeast m128ms series
Australia Southeast m128s series
Australia Southeast m32ts series
Australia Southeast m64 series
Australia Southeast m64-16ms series
Australia Southeast m64-32ms series
Australia Southeast m64ls series
Australia Southeast m64m series
Australia Southeast m64ms series
Australia Southeast m64s series
Australia Southeast m8ms series
West US 2 m128 series
West US 2 m128-32ms series
West US 2 m128-64ms series
West US 2 m128m series
West US 2 m128ms series
West US 2 m128s series
West US 2 m16ms series
West US 2 m32ls series
West US 2 m32ts series
West US 2 m64 series
West US 2 m64-16ms series
West US 2 m64-32ms series
West US 2 m64ls series
West US 2 m64m series
West US 2 m64ms series
West US 2 m64s series
West US 2 m8ms series
East Asia m128 series
East Asia m128-32ms series
East Asia m128-64ms series
East Asia m128m series
East Asia m128ms series
East Asia m128s series
East Asia m16ms series
East Asia m32ls series
East Asia m32ms series
East Asia m32ts series
East Asia m64 series
East Asia m64-16ms series
East Asia m64-32ms series
East Asia m64ls series
East Asia m64m series
East Asia m64ms series
East Asia m64s series
East Asia m8ms series
Southeast Asia l16s-v2 series
Southeast Asia l32s-v2 series
Southeast Asia l64s-v2 series
Southeast Asia l80s-v2 series
Southeast Asia l8s-v2 series
Southeast Asia m128 series
Southeast Asia m128-32ms series
Southeast Asia m128-64ms series
Southeast Asia m128m series
Southeast Asia m128ms series
Southeast Asia m128s series
Southeast Asia m16ms series
Southeast Asia m32ls series
Southeast Asia m32ms series
Southeast Asia m32ts series
Southeast Asia m64 series
Southeast Asia m64-16ms series
Southeast Asia m64-32ms series
Southeast Asia m64ls series
Southeast Asia m64m series
Southeast Asia m64ms series
Southeast Asia m64s series
Southeast Asia m8ms series
Japan East m128 series
Japan East m128-32ms series
Japan East m128-64ms series
Japan East m128m series
Japan East m128ms series
Japan East m128s series
Japan East m16ms series
Japan East m32ls series
Japan East m32ms series
Japan East m32ts series
Japan East m64 series
Japan East m64-16ms series
Japan East m64-32ms series
Japan East m64ls series
Japan East m64m series
Japan East m64ms series
Japan East m64s series
Japan East m8ms series
Japan West m128 series
Japan West m128-32ms series
Japan West m128-64ms series
Japan West m128m series
Japan West m128ms series
Japan West m128s series
Japan West m128s series
Japan West m16ms series
Japan West m32ls series
Japan West m32ms series
Japan West m32ts series
Japan West m64 series
Japan West m64-16ms series
Japan West m64-32ms series
Japan West m64ls series
Japan West m64m series
Japan West m64ms series
Japan West m8ms series
Central India m128 series
Central India m128-32ms series
Central India m128-64ms series
Central India m128m series
Central India m128s series
Central India m16ms series
Central India m32ls series
Central India m32ms series
Central India m32ts series
Central India m64 series
Central India m64-16ms series
Central India m64-32ms series
Central India m64ls series
Central India m64m series
Central India m64ms series
Central India m8ms series
South India m128 series
South India m128-32ms series
South India m128-64ms series
South India m128m series
South India m128s series
South India m16ms series
South India m32ls series
South India m32ms series
South India m32ts series
South India m64 series
South India m64-16ms series
South India m64-32ms series
South India m64ls series
South India m64m series
South India m64ms series
South India m8ms series
South India m8ms series
Canada Central m128 series
Canada Central m128-32ms series
Canada Central m128-64ms series
Canada Central m128m series
Canada Central m128ms series
Canada Central m128s series
Canada Central m128s series
Canada Central m16ms series
Canada Central m32ls series
Canada Central m32ms series
Canada Central m32ts series
Canada Central m64 series
Canada Central m64-16ms series
Canada Central m64-32ms series
Canada Central m64ls series
Canada Central m64m series
Canada Central m64ms series
Canada Central m64s series
Canada Central m8ms series
Canada East m128 series
Canada East m128-32ms series
Canada East m128-64ms series
Canada East m128m series
Canada East m128ms series
Canada East m16ms series
Canada East m32ls series
Canada East m32ms series
Canada East m32ts series
Canada East m64 series
Canada East m64-16ms series
Canada East m64-32ms series
Canada East m64ls series
Canada East m64m series
Canada East m64ms series
Canada East m64s series
Canada East m8ms series
UK South m128 series
UK South m128-32ms series
UK South m128-64ms series
UK South m128m series
UK South m128ms series
UK South m16ms series
UK South m32ls series
UK South m32ms series
UK South m32ts series
UK South m64 series
UK South m64-16ms series
UK South m64-32ms series
UK South m64ls series
UK South m64m series
UK South m64ms series
UK South m64s series
UK South m8ms series
UK West m128 series
UK West m128-32ms series
UK West m128-64ms series
UK West m128m series
UK West m128ms series
UK West m128s series
UK West m16ms series
UK West m32ls series
UK West m32ms series
UK West m32ts series
UK West m64 series
UK West m64-16ms series
UK West m64-32ms series
UK West m64ls series
UK West m64m series
UK West m64ms series
UK West m64s series
UK West m8ms series

**AWS Updates / November 21, 2018**

**New Instances**
Asia Seoul r5 series
Asia Seoul r5d series
Asia Singapore m5a series
Asia Singapore r5 series
Asia Singapore r5a series
Asia Singapore r5d series
Asia Tokyo r5 series
Asia Tokyo r5d series
Canada Central r5 series
Canada Central r5d series
EU Frankfurt r5 series
EU Frankfurt r5d series
EU Ireland m5a series
EU Ireland r5a series
EU Ireland r5d series
EU London i3 series
EU London r5 series
EU London r5d series
EU Paris r5 series
Pacific Sydney r5 series
Pacific Sydney r5d series
US California r5 series
US California r5d series
US GovCloud r5 series
US Ohio m5a series
US Ohio r5a series
US Oregon m5a series
US Oregon r5a series
US Virginia m5a series
US Virginia r5a series

**Azure Updates / November 21, 2018**

- **New Instances**
- **Updated Instances**

**New Instances**
Australia Central f16s series
Australia Central f1s series
Australia Central f2s series
| Australia Central f4s series          |
| Australia Central f8s series          |
| Australia Central 2 f16s series       |
| Australia Central 2 f1s series        |
| Australia Central 2 f2s series        |
| Australia Central 2 f4s series        |
| Australia Central 2 f8s series        |
| Australia East  f16s series           |
| Australia East f1s series             |
| Australia East f2s series             |
| Australia East f4s series             |
| Australia East f8s series             |
| Australia East m128-32ms series       |
| Australia East m128-64ms series       |
| Australia East m64-16ms series        |
| Australia East m64-32ms series        |
| Australia Southeast f16s series       |
| Australia Southeast f1s series        |
| Australia Southeast f2s series        |
| Australia Southeast f4s series        |
| Australia Southeast f8s series        |
| Australia Southeast m128-32ms series  |
| Australia Southeast m128-64ms series  |
| Australia Southeast m64-16ms series   |
| Australia Southeast m64-32ms series   |
| Brazil South f16s series              |
| Brazil South f1s series               |
| Brazil South f2s series               |
| Brazil South f4s series               |
| Brazil South f8s series               |
| Canada Central f16s series            |
| Canada Central f1s series             |
| Canada Central f2s series             |
| Canada Central f4s series             |
| Canada Central f8s series             |
| Canada Central m128-32ms series       |
| Canada Central m128-64ms series       |
| Canada Central m128ms series          |
| Canada Central m128s series           |
| Canada Central m16ms series           |
| Canada Central m32ls series           |
| Canada Central m32ms series           |
| Canada Central m32ts series           |
| Canada Central m64-16ms series        |
| Canada Central m64-32ms series        |
| Canada Central m641s series           |
| Canada Central m64ms series           |
| Canada Central m64s series            |
| Canada Central m8ms series            |
| Canada East f16s series               |
| Canada East f1s series                |
| Canada East f2s series                |
| Canada East f4s series                |
| Canada East f8s series                |
| Canada East m128-32ms series          |
| Canada East m128-64ms series          |
Canada East m128ms series
Canada East m128s series
Canada East m16ms series
Canada East m32ls series
Canada East m32ms series
Canada East m32ts series
Canada East m64-16ms series
Canada East m64-32ms series
Canada East m64ls series
Canada East m64ms series
Canada East m64s series
Central India f16s series
Central India f1s series
Central India f2s series
Central India f4s series
Central India f8s series
Central India m128-32s series
Central India m128-64ms series
Central India m64-16ms series
Central India m64-32ms series
Central US f16s series
Central US f1s series
Central US f2s series
Central US f4s series
Central US f8s series
East Asia f16s series
East Asia f1s series
East Asia f2s series
East Asia f4s series
East Asia f8s series
East Asia m128-32ms series
East Asia m128-64ms series
East Asia m128ms series
East Asia m128s series
East Asia m16ms series
East Asia m32ls series
East Asia m32ms series
East Asia m32ts series
East Asia m64-16ms series
East Asia m64-32ms series
East Asia m64ls series
East Asia m64ms series
East Asia m64s series
East Asia m8ms series
East US dc2s series
East US dc4s series
East US f16s series
East US f1s series
East US f2s series
East US f4s series
East US f8s series
East US m128-32ms series
East US m128-64ms series
East US m64-16ms series
East US m64-32ms series
East US 2 f16s series
East US 2 f1s series
East US 2 f2s series
East US 2 f4s series
East US 2 f8s series
France Central f16s series
France Central f1s series
France Central f2s series
France Central f4s series
France Central f8s series
France South f16s series
France South f1s series
France South f2s series
France South f4s series
France South f8s series
Germany Central f16s series
Germany Central f1s series
Germany Central f2s series
Germany Central f4s series
Germany Central f8s series
Germany Northeast f16s series
Germany Northeast f1s series
Germany Northeast f2s series
Germany Northeast f4s series
Germany Northeast f8s series
Japan East f16s series
Japan East f1s series
Japan East f2s series
Japan East f4s series
Japan East f8s series
Japan East m128-32ms series
Japan East m128-64ms series
Japan East m64-16ms series
Japan East m64-32ms series
Japan West f16s series
Japan West f1s series
Japan West f2s series
Japan West f4s series
Japan West f8s series
Japan West m128-32ms series
Japan West m128-64ms series
Japan West m64-16ms series
Japan West m64-32ms series
Korea Central f16s series
Korea Central f1s series
Korea Central f2s series
Korea Central f4s series
Korea Central f8s series
Korea South f16s series
Korea South f1s series
Korea South f2s series
Korea South f4s series
Korea South f8s series
North Central US f16s series
North Central US f1s series
North Central US f2s series
North Central US f4s series
North Central US f8s series
North Europe f16s series
North Europe f1s series
North Europe f2s series
North Europe f4s series
North Europe f8s series
North Europe m128-32ms series
North Europe m128-64ms series
North Europe m64-16ms series
North Europe m64-32ms series
South Central US f16s series
South Central US f1s series
South Central US f2s series
South Central US f4s series
South Central US f8s series
South India f16s series
South India f1s series
South India f2s series
South India f4s series
South India f8s series
South India m128-32ms series
South India m128-64ms series
South India m64-16ms series
South India m64-32ms series
Southeast Asia f16s series
Southeast Asia f1s series
Southeast Asia f2s series
Southeast Asia f4s series
Southeast Asia f8s series
UK South f16s series
UK South f1s series
UK South f2s series
UK South f4s series
UK South f8s series
UK West f16s series
UK West f1s series
UK West f2s series
UK West f4s series
UK West f8s series
UK West m128-64ms series
UK West m64-32ms series
US Gov Arizona f16s series
US Gov Arizona f1s series
US Gov Arizona f2s series
US Gov Arizona f4s series
US Gov Arizona f8s series
US Gov Arizona m128-32ms series
US Gov Arizona m128-64ms series
US Gov Arizona m64-16ms series
US Gov Arizona m64-32ms series
US Gov Texas f16s series
US Gov Texas f1s series
US Gov Texas f2s series
US Gov Texas f4s series
US Gov Texas f8s series
Updated Instances

Australia East f16s-v2 series
Australia East f2s-v2 series
Australia East f32s-v2 series
Australia East f4s-v2 series
Australia East f64s-v2 series
Australia East f72s-v2 series
Australia East f8s-v2 series
Brazil South f16s-v2 series
Brazil South f2s-v2 series
Brazil South f32s-v2 series
Brazil South f4s-v2 series
Brazil South f64s-v2 series
Brazil South f72s-v2 series
Brazil South f8s-v2 series
Canada Central f16s-v2 series
Canada Central f2s-v2 series
Canada Central f32s-v2 series
Canada Central f4s-v2 series
Canada Central f64s-v2 series
Canada Central f72s-v2 series
Canada Central f8s-v2 series
Central India f16s-v2 series
Central India f2s-v2 series
Central India f32s-v2 series
Central India f4s-v2 series
Central India f64s-v2 series
Central India f72s-v2 series
Central India f8s-v2 series
France Central f16s-v2 series
France Central f2s-v2 series
France Central f32s-v2 series
France Central f4s-v2 series
France Central f64s-v2 series
France Central f72s-v2 series
France Central f8s-v2 series
Japan East f16s-v2 series
Japan East f2s-v2 series
Japan East f32s-v2 series
Japan East f4s-v2 series
Japan East f64s-v2 series
Japan East f72s-v2 series
Japan East f8s-v2 series
Korea Central f16s-v2 series
Korea Central f2s-v2 series
Korea Central f32s-v2 series
Korea Central f4s-v2 series
Korea Central f64s-v2 series
Korea Central f72s-v2 series
Korea Central f8s-v2 series
North Central US f16s-v2 series
North Central US f2s-v2 series
North Central US f32s-v2 series
North Central US f4s-v2 series
North Central US f64s-v2 series
North Central US f72s-v2 series
North Central US f8s-v2 series
Southeast Asia f16s-v2 series
Southeast Asia f32s-v2 series
Southeast Asia f64s-v2 series
Southeast Asia f72s-v2 series
Southeast Asia f8s-v2 series
UK South f16s-v2 series
UK South f2s-v2 series
UK South f32s-v2 series
UK South f4s-v2 series
UK South f64s-v2 series
UK South f72s-v2 series
UK South f8s-v2 series
US Gov Arizona e16-4s-v3 series
US Gov Arizona e16-8s-v3 series
US Gov Arizona e16-v3 series
US Gov Arizona e16s-v3 series
US Gov Arizona e20-v3 series
US Gov Arizona e20s-v3 series
US Gov Arizona e32-16s-v3 series
US Gov Arizona e32-8s-v3 series
US Gov Arizona e32-v3 series
US Gov Arizona e32s-v3 series
US Gov Arizona e64-16s-v3 series
US Gov Arizona e64-32s-v3 series
US Gov Arizona e64-v3 series
US Gov Arizona e64s-v3 series
US Gov Arizona f16s-v2 series
US Gov Arizona f2s-v2 series
US Gov Arizona f32s-v2 series
US Gov Arizona f64s-v2 series
US Gov Arizona f72s-v2 series
US Gov Arizona h16m series
US Gov Arizona h8 series
US Gov Arizona m128ms series
US Gov Arizona m32ms series
US Gov Arizona m64ms series
US Gov Texas e16-4s-v3 series
US Gov Texas e16-8s-v3 series
US Gov Texas e16-v3 series
US Gov Texas e16s-v3 series
US Gov Texas e20-v3 series
US Gov Texas e20s-v3 series
US Gov Texas e32-16s-v3 series
US Gov Texas e32-8s-v3 series
US Gov Texas e32-v3 series
US Gov Texas e32s-v3 series
US Gov Texas e64-16s-v3 series
US Gov Texas e64-32s-v3 series
US Gov Texas e64-v3 series
US Gov Texas e64s-v3 series
US Gov Virginia m128-32ms series
US Gov Virginia m128-64ms series
US Gov Virginia m128ms series
US Gov Virginia m32ms series
US Gov Virginia m64-16ms series
US Gov Virginia m64-32ms series
US Gov Virginia m64ms series
West Europe f16s-v2 series
West Europe f2s-v2 series
West Europe f32s-v2 series
West Europe f4s-v2 series
West Europe f64s-v2 series
West Europe f72s-v2 series
West Europe f8s-v2 series
West US f16s-v2 series
West US f2s-v2 series
West US f32s-v2 series
West US f4s-v2 series
West US f64s-v2 series
West US f72s-v2 series
West US f8s-v2 series

**AWS Updates / October 2, 2018**

**New Instances**

Asia Seoul m5d series
Asia Seoul r5 series
Asia Seoul r5d series
Asia Singapore m5d series
Asia Tokyo c5d series
Asia Tokyo m5d series
Asia Tokyo r5 series
Canada Central r5 series
Canada Central r5d series
EU Frankfurt r5 series
EU Frankfurt r5d series
EU Ireland r5d series
EU London m5d series
EU London r5 series
EU London r5d series
GovCloud c5d series
GovCloud m5d series
GovCloud r5 series
Pacific Sydney c5d series
Pacific Sydney m5d series
Pacific Sydney r5 series
Pacific Sydney r5d series
US California r5 series
US California r5d series

**Azure Updates / October 2, 2018**

**New Instances**

Australia Central e20 series
Australia Central e20s series
Australia Central f16s series
Australia Central f2s series
Australia Central f32s series
Australia Central f4s series
Australia Central f64s series
Australia Central f72s series
Australia Central f8s series
Australia Central fs1 series
Australia Central fs16 series
Australia Central fs2 series
Australia Central fs4 series
Australia Central fs8 series
Australia Central 2 e20 series
Australia Central 2 e20s series
Australia Central 2 f16s series
Australia Central 2 f2s series
Australia Central 2 f32s series
Australia Central 2 f4s series
Australia Central 2 f64s series
Australia Central 2 f72s series
Australia Central 2 f8s series
Australia Central 2 fs1 series
Australia Central 2 fs16 series
Australia Central 2 fs2 series
Australia Central 2 fs4 series
Australia Central 2 fs8 series
<table>
<thead>
<tr>
<th>Australia East e20 series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia East e20s series</td>
</tr>
<tr>
<td>Australia East e64i series</td>
</tr>
<tr>
<td>Australia East e64is series</td>
</tr>
<tr>
<td>Australia East f16s series</td>
</tr>
<tr>
<td>Australia East f2s series</td>
</tr>
<tr>
<td>Australia East f32s series</td>
</tr>
<tr>
<td>Australia East f4s series</td>
</tr>
<tr>
<td>Australia East f64s series</td>
</tr>
<tr>
<td>Australia East f72s series</td>
</tr>
<tr>
<td>Australia East f8s series</td>
</tr>
<tr>
<td>Australia East fs1 series</td>
</tr>
<tr>
<td>Australia East fs16 series</td>
</tr>
<tr>
<td>Australia East fs2 series</td>
</tr>
<tr>
<td>Australia East fs4 series</td>
</tr>
<tr>
<td>Australia East fs8 series</td>
</tr>
<tr>
<td>Australia East gs1 series</td>
</tr>
<tr>
<td>Australia East gs2 series</td>
</tr>
<tr>
<td>Australia East gs3 series</td>
</tr>
<tr>
<td>Australia East gs4 series</td>
</tr>
<tr>
<td>Australia East gs5 series</td>
</tr>
<tr>
<td>Australia Southeast e20 series</td>
</tr>
<tr>
<td>Australia Southeast e20s series</td>
</tr>
<tr>
<td>Australia Southeast e64i series</td>
</tr>
<tr>
<td>Australia Southeast f16s series</td>
</tr>
<tr>
<td>Australia Southeast f2s series</td>
</tr>
<tr>
<td>Australia Southeast f32s series</td>
</tr>
<tr>
<td>Australia Southeast f4s series</td>
</tr>
<tr>
<td>Australia Southeast f64s series</td>
</tr>
<tr>
<td>Australia Southeast f72s series</td>
</tr>
<tr>
<td>Australia Southeast f8s series</td>
</tr>
<tr>
<td>Australia Southeast fs1 series</td>
</tr>
<tr>
<td>Australia Southeast fs16 series</td>
</tr>
<tr>
<td>Australia Southeast fs2 series</td>
</tr>
<tr>
<td>Australia Southeast fs4 series</td>
</tr>
<tr>
<td>Australia Southeast fs8 series</td>
</tr>
<tr>
<td>Brazil South e20 series</td>
</tr>
<tr>
<td>Brazil South e20s series</td>
</tr>
<tr>
<td>Brazil South e64i series</td>
</tr>
<tr>
<td>Brazil South f16s series</td>
</tr>
<tr>
<td>Brazil South f2s series</td>
</tr>
<tr>
<td>Brazil South f32s series</td>
</tr>
<tr>
<td>Brazil South f4s series</td>
</tr>
<tr>
<td>Brazil South f64s series</td>
</tr>
<tr>
<td>Brazil South f72s series</td>
</tr>
<tr>
<td>Brazil South f8s series</td>
</tr>
<tr>
<td>Brazil South fs1 series</td>
</tr>
<tr>
<td>Brazil South fs16 series</td>
</tr>
<tr>
<td>Brazil South fs2 series</td>
</tr>
<tr>
<td>Brazil South fs4 series</td>
</tr>
<tr>
<td>Brazil South fs8 series</td>
</tr>
<tr>
<td>Canada Central e20 series</td>
</tr>
<tr>
<td>Canada Central e20s series</td>
</tr>
<tr>
<td>Canada Central e64i series</td>
</tr>
<tr>
<td>Canada Central f16s series</td>
</tr>
<tr>
<td>Canada Central f2s series</td>
</tr>
</tbody>
</table>
Canada Central f32s series
Canada Central f4s series
Canada Central f64s series
Canada Central f72s series
Canada Central f8s series
Canada Central fs1 series
Canada Central fs16 series
Canada Central fs2 series
Canada Central fs4 series
Canada Central fs8 series
Canada Central gs1 series
Canada Central gs2 series
Canada Central gs3 series
Canada Central gs4 series
Canada Central gs5 series
Canada East e20 series
Canada East e20s series
Canada East e64i series
Canada East e64is series
Canada East f16s series
Canada East f2s series
Canada East f32s series
Canada East f4s series
Canada East f64s series
Canada East f72s series
Canada East f8s series
Canada East fs1 series
Canada East fs16 series
Canada East fs2 series
Canada East fs4 series
Canada East fs8 series
Canada East gs1 series
Canada East gs2 series
Canada East gs3 series
Canada East gs4 series
Canada East gs5 series
Central India e20 series
Central India e20s series
Central India f16s series
Central India f2s series
Central India f32s series
Central India f4s series
Central India f64s series
Central India f72s series
Central India f8s series
Central India fs1 series
Central India fs16 series
Central India fs2 series
Central India fs4 series
Central India fs8 series
Central US e20 series
Central US e20s series
Central US e64i series
Central US f16s series
Central US f2s series
Central US f32s series
Central US f4s series
Central US f64s series
Central US f72s series
Central US f8s series
Central US fs1 series
Central US fs16 series
Central US fs2 series
Central US fs4 series
Central US fs8 series
East Asia e20 series
East Asia e20s series
East Asia e64i series
East Asia f16s series
East Asia f2s series
East Asia f32s series
East Asia f4s series
East Asia f64s series
East Asia f72s series
East Asia f8s series
East Asia fs1 series
East Asia fs16 series
East Asia fs2 series
East Asia fs4 series
East Asia fs8 series
East US e20 series
East US e20s series
East US e64i series
East US f16s series
East US f2s series
East US f32s series
East US f4s series
East US f64s series
East US f72s series
East US f8s series
East US fs1 series
East US fs16 series
East US fs2 series
East US fs4 series
East US fs8 series
East US 2 e20 series
East US 2 e20s series
East US 2 e64i series
East US 2 f16s series
East US 2 f2s series
East US 2 f32s series
East US 2 f4s series
East US 2 f64s series
East US 2 f72s series
East US 2 f8s series
East US 2 fs1 series
East US 2 fs16 series
East US 2 fs2 series
East US 2 fs4 series
East US 2 fs8 series
East US 2 gs1 series
East US 2 gs2 series
East US 2 gs3 series
East US 2 gs4 series
East US 2 gs5 series
France Central e20 series
France Central e20s series
France Central e64i series
France Central f16s series
France Central f2s series
France Central f32s series
France Central f4s series
France Central f64s series
France Central f72s series
France Central f8s series
France Central fs1 series
France Central fs16 series
France Central fs2 series
France Central fs4 series
France Central fs8 series
France South e20 series
France South e20s series
France South e64i series
France South f16s series
France South f2s series
France South f32s series
France South f4s series
France South f64s series
France South f72s series
France South f8s series
France South fs1 series
France South fs16 series
France South fs2 series
France South fs4 series
France South fs8 series
Germany Central e64i series
Germany Central fs1 series
Germany Central fs16 series
Germany Central fs2 series
Germany Central fs4 series
Germany Central fs8 series
Germany Central gs1 series
Germany Central gs2 series
Germany Central gs3 series
Germany Central gs4 series
Germany Central gs5 series
Germany Northeast e64i series
Germany Northeast fs1 series
Germany Northeast fs16 series
Germany Northeast fs2 series
Germany Northeast fs4 series
Germany Northeast fs8 series
Japan East e20 series
Japan East e20s series
Japan East e64i series
Japan East f16s series
Japan East f2s series
Japan East f32s series
Japan East f4s series
Japan East f64s series
Japan East f72s series
Japan East f8s series
Japan East fs1 series
Japan East fs16 series
Japan East fs2 series
Japan East fs4 series
Japan East fs8 series
Japan East gs1 series
Japan East gs2 series
Japan East gs3 series
Japan East gs4 series
Japan East gs5 series
Japan West e20 series
Japan West e20s series
Japan West e64i series
Japan West f16s series
Japan West f2s series
Japan West f32s series
Japan West f4s series
Japan West f64s series
Japan West f72s series
Japan West f8s series
Japan West fs1 series
Japan West fs16 series
Japan West fs2 series
Japan West fs4 series
Japan West fs8 series
Korea Central e20 series
Korea Central e20s series
Korea Central e64i series
Korea Central f16s series
Korea Central f2s series
Korea Central f32s series
Korea Central f4s series
Korea Central f64s series
Korea Central f72s series
Korea Central f8s series
Korea Central fs1 series
Korea Central fs16 series
Korea Central fs2 series
Korea Central fs4 series
Korea Central fs8 series
Korea South e20 series
Korea South e20s series
Korea South e64i series
Korea South f16s series
Korea South f2s series
Korea South f32s series
Korea South f4s series
Korea South f64s series
Korea South f72s series
Korea South f8s series
Korea South fs1 series
Korea South fs16 series
Korea South fs2 series
Korea South fs4 series
Korea South fs8 series
North Central US e20 series
North Central US e20s series
North Central US e64i series
North Central US f16s series
North Central US f2s series
North Central US f32s series
North Central US f4s series
North Central US f64s series
North Central US f72s series
North Central US f8s series
North Central US fs1 series
North Central US fs16 series
North Central US fs2 series
North Central US fs4 series
North Central US fs8 series
North Europe e20 series
North Europe e20s series
North Europe e64i series
North Europe f16s series
North Europe f2s series
North Europe f32s series
North Europe f4s series
North Europe f64s series
North Europe f72s series
North Europe f8s series
North Europe fs1 series
North Europe fs16 series
North Europe fs2 series
North Europe fs4 series
North Europe fs8 series
North Europe m128ms series
North Europe m128s series
North Europe m16ms series
North Europe m32ls series
North Europe m32ms series
North Europe m32ts series
North Europe m64ls series
North Europe m64ms series
North Europe m64s series
North Europe m8ms series
South Central US e20 series
South Central US e20s series
South Central US e64i series
South Central US f16s series
South Central US f2s series
South Central US f32s series
South Central US f4s series
South Central US f64s series
South Central US f72s series
South Central US f8s series
South Central US fs1 series
South Central US fs16 series
South Central US fs2 series
South Central US fs4 series
South Central US fs8 series
South India e20 series
South India e20s series
South India e64i series
South India f16s series
South India f2s series
South India f32s series
South India f4s series
South India f64s series
South India f72s series
South India f8s series
South India fs1 series
South India fs16 series
South India fs2 series
South India fs4 series
South India fs8 series
Southeast Asia e20 series
Southeast Asia e20s series
Southeast Asia e64i series
Southeast Asia f16s series
Southeast Asia f2s series
Southeast Asia f32s series
Southeast Asia f4s series
Southeast Asia f64s series
Southeast Asia f72s series
Southeast Asia f8s series
Southeast Asia fs1 series
Southeast Asia fs16 series
Southeast Asia fs2 series
Southeast Asia fs4 series
Southeast Asia fs8 series
Southeast Asia gs1 series
Southeast Asia gs2 series
Southeast Asia gs3 series
Southeast Asia gs4 series
Southeast Asia gs5 series
UK South e20 series
UK South e20s series
UK South e64i series
UK South f16s series
UK South f2s series
UK South f32s series
UK South f4s series
UK South f64s series
UK South f72s series
UK South f8s series
UK South fs1 series
UK South fs16 series
UK South fs2 series
UK South fs4 series
UK South fs8 series
UK South gs1 series
UK South gs2 series
UK South gs3 series
UK South gs4 series
UK South gs5 series
UK West e20 series
UK West e20s series
UK West e64i series
UK West f16s series
UK West f2s series
UK West f32s series
UK West f4s series
UK West f64s series
UK West f72s series
UK West f8s series
UK West fs1 series
UK West fs16 series
UK West fs2 series
UK West fs4 series
UK West fs8 series
US Gov Arizona d16 series
US Gov Arizona d16s series
US Gov Arizona d2 series
US Gov Arizona d2s series
US Gov Arizona d32 series
US Gov Arizona d32s series
US Gov Arizona d4 series
US Gov Arizona d4s series
US Gov Arizona d64 series
US Gov Arizona d64s series
US Gov Arizona d8 series
US Gov Arizona d8s series
US Gov Arizona e16 series
US Gov Arizona e16s series
US Gov Arizona e2 series
US Gov Arizona e20 series
US Gov Arizona e20s series
US Gov Arizona e2s series
US Gov Arizona e32 series
US Gov Arizona e32s series
US Gov Arizona e4 series
US Gov Arizona e4s series
US Gov Arizona e64 series
US Gov Arizona e64s series
US Gov Arizona e8 series
US Gov Arizona e8s series
US Gov Arizona f16s series
US Gov Arizona f2s series
US Gov Arizona f32s series
US Gov Arizona f4s series
US Gov Arizona f64s series
US Gov Arizona f72s series
US Gov Arizona f8s series
US Gov Arizona fs1 series
US Gov Arizona fs16 series
US Gov Arizona fs2 series
US Gov Arizona fs4 series
US Gov Arizona fs8 series
US Gov Texas e20 series
US Gov Texas e20s series
US Gov Texas f16s series
US Gov Texas f2s series
US Gov Texas f32s series
US Gov Texas f4s series
US Gov Texas f64s series
US Gov Texas f72s series
US Gov Texas f8s series
US Gov Texas fs1 series
US Gov Texas fs16 series
US Gov Texas fs2 series
US Gov Texas fs4 series
US Gov Texas fs8 series
US Gov Virginia f16s series
US Gov Virginia f2s series
US Gov Virginia f32s series
US Gov Virginia f4s series
US Gov Virginia f64s series
US Gov Virginia f72s series
US Gov Virginia f8s series
US Gov Virginia fs1 series
US Gov Virginia fs16 series
US Gov Virginia fs2 series
US Gov Virginia fs4 series
US Gov Virginia fs8 series
US Gov Virginia gs1 series
US Gov Virginia gs2 series
US Gov Virginia gs3 series
US Gov Virginia gs4 series
US Gov Virginia gs5 series
West Central US f16s series
West Central US f2s series
West Central US f32s series
West Central US f4s series
West Central US f64s series
West Central US f72s series
West Central US f8s series
West Central US fs1 series
West Central US fs16 series
West Central US fs2 series
West Central US fs4 series
West Central US fs8 series
West Europe e20 series
West Europe e20s series
West Europe e64i series
West Europe f16s series
West Europe f2s series
West Europe f32s series
West Europe f4s series
West Europe f64s series
West Europe f72s series
West Europe f8s series
West Europe fs1 series
West Europe fs16 series
West Europe fs2 series
West Europe fs4 series
West Europe fs8 series
West Europe gs1 series
West Europe gs2 series
West Europe gs3 series
West Europe gs4 series
West Europe gs5 series
West India e20 series
West India e20s series
West India e64i series
West India f16s series
West India f2s series
West India f32s series
West India f4s series
West India f64s series
West India f72s series
West India f8s series
West India fs1 series
West India fs16 series
West India fs2 series
West India fs4 series
West India fs8 series
West US e20 series
West US e20s series
West US e64i series
West US f16s series
West US f2s series
West US f32s series
West US f4s series
West US f64s series
West US f72s series
West US f8s series
West US fs1 series
West US fs16 series
West US fs2 series
West US fs4 series
West US fs8 series
West US gs1 series
West US gs2 series
West US gs3 series
West US gs4 series
West US gs5 series
West US 2 e20 series
West US 2 e20s series
West US 2 e64i series
West US 2 f16s series
West US 2 f2s series
West US 2 f32s series
West US 2 f4s series
West US 2 f64s series
West US 2 f72s series
West US 2 f8s series
West US 2 fs1 series
West US 2 fs16 series
West US 2 fs2 series
West US 2 fs4 series
West US 2 fs8 series
West US 2 gs1 series
West US 2 gs2 series
West US 2 gs3 series
West US 2 gs4 series
West US 2 gs5 series

**AWS Updates / August 23, 2018**

- **New Locations**
- **Updated Instances**

**New Locations**
asia-osaka

**Updated Instances**
Asia Mumbai m4 series
Asia Mumbai m5 series
Asia Mumbai t2 series
Asia Mumbai x1 series
Asia Seoul c5d series
Asia Seoul m4 series
Asia Seoul m5 series
Asia Seoul t2 series
Asia Seoul x1 series
Asia Singapore c5d series
Asia Singapore m4 series
Asia Singapore m5 series
Asia Singapore t2 series
Asia Singapore t3 series
Asia Singapore x1 series
Asia Singapore z1d series
Asia Tokyo m4 series
Asia Tokyo m5 series
Asia Tokyo t2 series
Asia Tokyo t3 series
Asia Tokyo x1 series
Asia Tokyo z1d series
Canada Central c5d series
Canada Central m4 series
Canada Central m5 series
Canada Central m5d series
Canada Central t2 series
Canada Central t3 series
Canada Central x1 series
EU Frankfurt c5d series
EU Frankfurt i3 series
EU Frankfurt m4 series
EU Frankfurt m5 series
EU Frankfurt m5d series
EU Frankfurt t2 series
EU Frankfurt t3 series
EU Frankfurt x1 series
EU Frankfurt x1e series
EU Ireland c5d series
EU Ireland i3 series
EU Ireland m4 series
EU Ireland m5 series
EU Ireland m5d series
EU Ireland r5 series
EU Ireland t2 series
EU Ireland t3 series
EU Ireland x1 series
EU Ireland z1d series
EU London c5d series
EU London m4 series
EU London m5 series
EU London t2 series
EU London t3 series
EU London x1 series
EU Paris m5 series
EU Paris t2 series
EU Paris x1 series
GovCloud c5 series
GovCloud m4 series
GovCloud m5 series
GovCloud t2 series
GovCloud x1 series
GovCloud x1e series
Pacific Sydney m4 series
Pacific Sydney m5 series
Pacific Sydney t2 series
Pacific Sydney t3 series
Pacific Sydney x1 series
South America m4 series
South America m5 series
South America t2 series
South America t3 series
South America x1 series
US California c5d series
US California m4 series
US California m5 series
US California m5d series
US California t2 series
US California t3 series
US California z1d series
US Ohio c5d series
US Ohio i3 series
US Ohio m4 series
US Ohio m5 series
US Ohio m5d series
US Ohio r5 series
US Ohio r5d series
US Ohio t2 series
US Ohio t3 series
US Ohio x1 series
US Oregon c5d series
US Oregon i3 series
US Oregon m4 series
US Oregon m5 series
US Oregon m5d series
US Oregon r5 series
US Oregon r5d series
US Oregon t2 series
US Oregon t3 series
US Oregon x1 series
US Oregon z1d series
US Virginia c5d series
US Virginia i3 series
US Virginia m4 series
US Virginia m5 series
US Virginia m5d series
US Virginia r5 series
US Virginia r5d series
US Virginia t2 series
US Virginia t3 series
US Virginia x1 series
US Virginia z1d series

Azure Updates / August 23, 2018

- New Instances
- Updated Instances

New Instances
Australia Central a1 series
Australia Central a2 series
Australia Central a2m series
Australia Central a4 series
Australia Central a4m series
Australia Central a8 series
Australia Central a8m series
Australia Central d1 series
Australia Central d11 series
Australia Central d12 series
Australia Central d13 series
Australia Central d14 series
Australia Central d15 series
Australia Central d16 series
Australia Central d16s series
Australia Central d2 series
Australia Central d2s series
Australia Central d3 series
Australia Central d32 series
Australia Central d32s series
Australia Central d4 series
Australia Central d4s series
Australia Central d5 series
Australia Central d64 series
Australia Central d64s series
Australia Central d8 series
Australia Central d8s series
Australia Central ds1 series
Australia Central ds11 series
Australia Central ds12 series
Australia Central ds13 series
Australia Central ds14 series
Australia Central ds15 series
Australia Central ds2 series
Australia Central ds3 series
Australia Central ds4 series
Australia Central ds5 series
Australia Central e16 series
Australia Central e16s series
Australia Central e2 series
Australia Central e2s series
Australia Central e32 series
Australia Central e32s series
Australia Central e4 series
Australia Central e4s series
Australia Central e64 series
Australia Central e64s series
Australia Central e8 series
Australia Central e8s series
Australia Central f1 series
Australia Central f16 series
Australia Central f16s series
Australia Central f2 series
Australia Central f2s series
Australia Central f32 series
Australia Central f4 series
Australia Central f64 series
Australia Central f72 series
Australia Central f8 series
Australia Central f8s series
France South a1 series
France South a2 series
France South a2m series
France South a4 series
France South a4m series
France South a8 series
France South a8m series
France South d1 series
France South d11 series
France South d12 series
France South d13 series
France South d14 series
France South d15 series
France South d16 series
France South d16s series
France South d2 series
France South d2s series
France South d3 series
France South d32 series
France South d32s series
France South d4 series
France South d4s series
France South d5 series
France South d64 series
France South d64s series
France South d8 series
France South d8s series
France South ds1 series
France South ds11 series
France South ds12 series
France South ds13 series
France South ds14 series
France South ds15 series
France South ds2 series
France South ds3 series
France South ds4 series
France South ds5 series
France South e16 series
France South e2 series
France South e32 series
France South e4 series
France South e64 series
France South e64i series
France South e64is series
France South e8 series
France South f1 series
France South f16 series
France South f2 series
France South f4 series
France South f8 series
Australia Central a1 series
Australia Central a2 series
Australia Central a2m series
Australia Central a4 series
Australia Central a4m series
Australia Central a8 series
Australia Central a8m series
Australia Central d1 series
Australia Central d11 series
Australia Central d12 series
Australia Central d13 series
Australia Central d14 series
Australia Central d15 series
Australia Central d16 series
Australia Central d16s series
Australia Central d2 series
Australia Central d2s series
Australia Central d3 series
Australia Central d32 series
Australia Central d32s series
Australia Central d4 series
Australia Central d4s series
Australia Central d5 series
Australia Central d64 series
Australia Central d64s series
Australia Central d8 series
Australia Central d8s series
Australia Central ds1 series
Australia Central ds11 series
Australia Central ds12 series
Australia Central ds13 series
Australia Central ds14 series
Australia Central ds15 series
Australia Central ds2 series
Australia Central ds3 series
Australia Central ds4 series
Australia Central ds5 series
Australia Central e16 series
Australia Central e16s series
Australia Central e2 series
Australia Central e2s series
Australia Central e32 series
Australia Central e32s series
Australia Central e4 series
Australia Central e4s series
Australia Central e64 series
Australia Central e64s series
Australia Central e8 series
Australia Central e8s series
Australia Central f1 series
Australia Central f16 series
Australia Central f2 series
Australia Central f4 series
Australia Central f8 series
France Central a1 series
France Central a2 series
France Central a2m series
France Central a4 series
France Central a4m series
France Central a8 series
France Central a8m series
France Central d1 series
France Central d11 series
France Central d12 series
France Central d13 series
France Central d14 series
France Central d15 series
France Central d16 series
France Central d16s series
France Central d2 series
France Central d2s series
France Central d3 series
France Central d32 series
France Central d32s series
France Central d4 series
France Central d4s series
France Central d5 series
France Central d64 series
France Central d64s series
France Central d8 series
France Central d8s series
France Central ds1 series
France Central ds11 series
France Central ds12 series
France Central ds13 series
France Central ds14 series
France Central ds15 series
France Central ds2 series
France Central ds3 series
France Central ds4 series
France Central ds5 series
France Central e16 series
France Central e2 series
France Central e32 series
France Central e4 series
France Central e64 series
France Central e64i series
France Central e64is series
France Central e8 series
France Central f1 series
France Central f16 series
France Central f2 series
France Central f4 series
France Central f8 series
Australia East d1 series
Australia East d11 series
Australia East d12 series
Australia East d13 series
Australia East d2 series
Australia East d3 series
Australia East d4 series
Australia East ds1 series
Australia East ds11 series
Australia East ds12 series
Australia East ds13 series
Australia East ds14 series
Australia East ds2 series
Australia East ds3 series
Australia East ds4 series
Australia East e16 series
Australia East e16s series
Australia East e2 series
Australia East e32 series
Australia East e4 series
Australia East e64 series
Australia East e64i series
Australia East e8 series
Australia East f16 series
Australia East f4 series
Australia East f8 series
Australia East gs4 series
Australia East gs5 series
Australia East m128ms series
Australia East m128s series
Australia East m16ms series
Australia East m32ls series
Australia East m32ls series
Australia East m32ms series
Australia East m32ts series
Australia East m64ls series
Australia East m64ms series
Australia East m64s series
Australia East m8ms series
Australia Southeast d1 series
Australia Southeast d11 series
Australia Southeast d12 series
Australia Southeast d13 series
Australia Southeast d16s series
Australia Southeast d2 series
Australia Southeast d2s series
Australia Southeast d3 series
Australia Southeast d32s series
Australia Southeast d4 series
Australia Southeast d4s series
Australia Southeast d64s series
Australia Southeast d8s series
Australia Southeast ds1 series
Australia Southeast ds11 series
Australia Southeast ds12 series
Australia Southeast ds13 series
Australia Southeast ds14 series
Australia Southeast ds2 series
Australia Southeast ds3 series
Australia Southeast ds4 series
Australia Southeast e16 series
Australia Southeast e16s series
Australia Southeast e2 series
Australia Southeast e32 series
Australia Southeast e4 series
Australia Southeast e64 series
Australia Southeast e641 series
Australia Southeast e64is series
Australia Southeast e8 series
Australia Southeast f16 series
Australia Southeast f4 series
Australia Southeast f8 series
Australia Southeast m128ms series
Australia Southeast m128s series
Australia Southeast m16ms series
Australia Southeast m32ls series
Australia Southeast m32ms series
Australia Southeast m32ts series
Australia Southeast m64ls series
Australia Southeast m64ms series
Australia Southeast m64s series
Australia Southeast m8ms series
Brazil South d1 series
Brazil South d11 series
Brazil South d12 series
Brazil South d13 series
Brazil South d16 series
Brazil South d16s series
Brazil South d2s series
Brazil South d32s series
Brazil South d4s series
Brazil South d64s series
Brazil South d8s series
Brazil South ds1 series
Brazil South ds11 series
Brazil South ds12 series
Brazil South ds13 series
Brazil South ds14 series
Brazil South e16 series
Brazil South e16s series
Brazil South e2 series
Brazil South e2s series
Brazil South e32 series
Brazil South e32s series
Brazil South e4 series
Brazil South e4s series
Brazil South e64 series
Brazil South e64i series
Brazil South e64is series
Brazil South e64s series
Brazil South e8 series
Brazil South e8s series
Brazil South f1 series
Brazil South f2 series
Brazil South f4 series
Brazil South f8 series
Canada Central d1 series
Canada Central d11 series
Canada Central d12 series
Canada Central d13 series
Canada Central d15 series
Canada Central d16 series
Canada Central d2 series
Canada Central d2s series
Canada Central d3 series
Canada Central d32s series
Canada Central d4 series
Canada Central d4s series
Canada Central d5 series
Canada Central d64s series
Canada Central d8s series
Canada Central ds1 series
Canada Central ds11 series
Canada Central ds12 series
Canada Central ds13 series
Canada Central ds14 series
Canada Central ds15 series
Canada Central ds2 series
Canada Central ds3 series
Canada Central ds4 series
Canada Central ds5 series
Canada Central e16 series
Canada Central e16s series
Canada Central e2 series
Canada Central e32 series
Canada Central e4 series
Canada Central e64 series
Canada Central e64i series
Canada Central e64is series
Canada Central e8 series
Canada Central f16 series
Canada Central f2 series
Canada Central f2 series
Canada Central f8 series
Canada Central gs4 series
Canada Central gs5 series
Canada East d1 series
Canada East d11 series
Canada East d12 series
Canada East d13 series
Canada East d15 series
Canada East d16s series
Canada East d2 series
Canada East d2s series
Canada East d3 series
Canada East d32s series
Canada East d4 series
Canada East d4s series
Canada East d64s series
Canada East d8s series
Canada East ds1 series
Canada East ds11 series
Canada East ds12 series
Canada East ds13 series
Canada East ds14 series
Canada East ds15 series
Canada East ds2 series
Canada East ds3 series
Canada East ds4 series
Canada East e16 series
Canada East e16s series
Canada East e2 series
Canada East e32 series
Canada East e4 series
Canada East e64 series
Canada East e64i series
Canada East e64is series
Canada East e8 series
Canada East f16 series
Canada East f2 series
Canada East f8 series
Canada East gs4 series
Canada East gs5 series
Central India d1 series
Central India d11 series
Central India ds1 series
Central India ds11 series
Central India ds12 series
Central India ds13 series
Central India ds14 series
Central India e16 series
Central India e16s series
Central India e2 series
Central India e32 series
Central India e4 series
Central India e64 series
Central India e8 series
Central India f1 series
Central India f16 series
Central India f4 series
Central India f8 series
Central India m128ms series
Central India m128s series
Central India m16ms series
Central India m32ls series
Central India m32ms series
Central India m32ts series
Central India m64ls series
Central India m64ms series
Central India m64s series
Central India m8ms series
Central US d1-v2 series
Central US d11 series
Central US d12 series
Central US d13 series
Central US d2 series
Central US d3 series
Central US d4 series
Central US ds1-v2 series
Central US ds11 series
Central US ds11-1-v2 series
Central US ds12 series
Central US ds12-1-v2 series
Central US ds12-2-v2 series
Central US ds13 series
Central US ds13-2-v2 series
Central US ds13-4-v2 series
Central US ds14-4-v2 series
Central US ds14-8-v2 series
Central US ds2 series
Central US ds3 series
Central US ds4 series
Central US e16 series
Central US e16-4s-v3 series
Central US e16-8s-v3 series
Central US e16-v3 series
Central US e16s series
Central US e16s-v3 series
Central US e2 series
Central US e2-v3 series
Central US e32 series
Central US e32-16s-v3 series
Central US e32-8s-v3 series
Central US e32-v3 series
Central US e4 series
Central US e4-2s-v3 series
Central US e4-v3 series
Central US e64 series
Central US e64-16s-v3 series
Central US e64-32s-v3 series
Central US e64-v3 series
Central US e64i series
Central US e64i-v3-1 series
Central US e64is series
Central US e64is-v3-1 series
Central US e8 series
Central US e8-2s-v3 series
Central US e8-v3 series
Central US f1 series
Central US f16 series
Central US f2 series
East Asia d1 series
East Asia d11 series
East Asia d12 series
East Asia d13 series
East Asia d16s series
East Asia d2 series
East Asia d2s series
East Asia d3 series
East Asia d32s series
East Asia d4 series
East Asia d4s series
East Asia d64s series
East Asia d8s series
East Asia ds1 series
East Asia ds11 series
East Asia ds12 series
East Asia ds13 series
East Asia ds14 series
East Asia ds2 series
East Asia ds3 series
East Asia ds4 series
East Asia e16 series
East Asia e16s series
East Asia e2 series
East Asia e32 series
East Asia e4 series
East Asia e64 series
East Asia e64s series
East Asia e64is series
East Asia e8 series
East Asia f16 series
East Asia f4 series
East Asia f8 series
East US d1 series
East US d11 series
East US d12 series
East US d13 series
East US d2 series
East US d3 series
East US d4 series
East US ds1 series
East US ds11 series
East US ds12 series
East US ds13 series
East US ds14 series
East US ds2 series
East US ds3 series
East US ds4 series
East US e16 series
East US e16s series
East US e2 series
East US e32 series
East US e4 series
East US e64 series
East US e64i series
East US e64is series
East US e8 series
East US f2 series
East US h16 series
East US h16m series
East US m128ms series
East US m128s series
East US m16ms series
East US m32ls series
East US m32ms series
East US m64ls series
East US m64ms series
East US m64s series
East US m8ms series
East US 2 d1 series
East US 2 d11 series
East US 2 d12 series
East US 2 d13 series
East US 2 d14 series
East US 2 d15 series
East US 2 d16 series
East US 2 d16s series
East US 2 d2 series
East US 2 d2s series
East US 2 d3 series
East US 2 d32 series
East US 2 d32s series
East US 2 d4 series
East US 2 d4s series
East US 2 d64 series
East US 2 d64s series
East US 2 d8 series
East US 2 d8s series
East US 2 ds1 series
East US 2 ds11 series
East US 2 ds12 series
East US 2 ds13 series
East US 2 ds14 series
East US 2 ds15 series
East US 2 ds2 series
East US 2 ds3 series
East US 2 ds4 series
East US 2 e16 series
East US 2 e16s series
East US 2 e2 series
East US 2 e2s series
East US 2 e32 series
East US 2 e32s series
East US 2 e4 series
East US 2 e4s series
East US 2 e64 series
East US 2 e64i series
East US 2 e64is series
East US 2 e64s series
East US 2 e8 series
East US 2 e8s series
East US 2 f1 series
East US 2 f16 series
East US 2 f16 series
East US 2 f2 series
East US 2 f2 series
East US 2 f32 series
East US 2 f4 series
East US 2 f4 series
East US 2 f64 series
East US 2 f72 series
East US 2 f8 series
East US 2 f8 series
East US 2 gs4 series
East US 2 gs5 series
East US 2 m128 series
East US 2 m128ms series
East US 2 m128s series
East US 2 m16ms series
East US 2 m32ls series
East US 2 m32ms series
East US 2 m32ts series
East US 2 m64 series
East US 2 m64ls series
East US 2 m64ms series
East US 2 m64s series
East US 2 m8ms series
Germany Central d1 series
Germany Central d11 series
Germany Central d12 series
Germany Central d13 series
Germany Central d15 series
Germany Central d16 series
Germany Central d16s series
Germany Central d2s series
Germany Central d32s series
Germany Central d4s series
Germany Central d64s series
Germany Central d8s series
Germany Central ds1 series
Germany Central ds11 series
Germany Central ds12 series
Germany Central ds13 series
Germany Central ds14 series
Germany Central ds15 series
Germany Central e16 series
Germany Central e16s series
Germany Central e32 series
Germany Central e4 series
Germany Central e64 series
Germany Central e64i series
Germany Central e64is series
Germany Central e8 series
Germany Central f1 series
Germany Central f16 series
Germany Central f2 series
Germany Central gs4 series
Germany Central gs5 series
Germany Northeast d1 series
Germany Northeast d11 series
Germany Northeast d12 series
Germany Northeast d13 series
Germany Northeast d15 series
Germany Northeast d16 series
Germany Northeast d16s series
Germany Northeast d2s series
Germany Northeast d32s series
Germany Northeast d4s series
Germany Northeast d64s series
Germany Northeast d8s series
Germany Northeast ds1 series
Germany Northeast ds11 series
Germany Northeast ds12 series
Germany Northeast ds13 series
Germany Northeast ds14 series
Germany Northeast ds15 series
Germany Northeast e16 series
Germany Northeast e16s series
Germany Northeast e32 series
Germany Northeast e4 series
Germany Northeast e64 series
Germany Northeast e64i series
Germany Northeast e64is series
Germany Northeast e8 series
Germany Northeast f1 series
Germany Northeast f16 series
Germany Northeast f2 series
Japan East d1 series
Japan East d11 series
Japan East d12 series
Japan East d13 series
Japan East d16 series
Japan East d2 series
Japan East d3 series
Japan East d4 series
Japan East ds1 series
Japan East ds11 series
Japan East ds12 series
Japan East ds13 series
Japan East ds14 series
Japan East ds2 series
Japan East ds3 series
Japan East ds4 series
Japan East e16 series
Japan East e16s series
Japan East e32 series
Japan East e4 series
Japan East e64 series
Japan East e64i series
Japan East e64is series
Japan East e8 series
Japan East f16 series
Japan East f2 series
Japan East f32 series
Japan East f4 series
Japan East f64 series
Japan East f72 series
Japan East f8 series
Japan East gs4 series
Japan East gs5 series
Japan East m128ms series
Japan East m128s series
Japan East m16ms series
Japan East m32ls series
Japan East m32ms series
Japan East m32ts series
Japan East m64ls series
Japan East m64ms series
Japan East m64s series
Japan East m64s series
Japan East m8ls series
Japan West d1 series
Japan West d11 series
Japan West d12 series
Japan West d13 series
Japan West d2 series
Japan West d3 series
Japan West d4 series
Japan West ds1 series
Japan West ds11 series
Japan West ds12 series
Japan West ds13 series
Japan West ds14 series
Japan West ds2 series
Japan West ds3 series
Japan West ds4 series
Japan West e16 series
Japan West e16s series
Japan West e2 series
Japan West e32 series
Japan West e4 series
Japan West e64 series
Japan West e64i series
Japan West e64is series
Japan West e8 series
Japan West f16 series
Japan West f2 series
Japan West f32 series
Japan West f4 series
Japan West f64 series
Japan West f72 series
Japan West f8 series
Japan West m128ms series
Japan West m128s series
Japan West m16ms series
Japan West m32ls series
Japan West m32ms series
Japan West m32ts series
Japan West m64ls series
Japan West m64ms series
Japan West m64s series
Japan West m8ms series
Korea Central d1 series
Korea Central d3 series
Korea Central ds1 series
Korea Central ds11 series
Korea Central ds12 series
Korea Central ds13 series
Korea Central ds14 series
Korea Central ds3 series
Korea Central e16 series
Korea Central e16s series
Korea Central e2 series
Korea Central e32 series
Korea Central e4 series
Korea Central e64 series
Korea Central e64i series
Korea Central e64is series
Korea Central e8 series
Korea Central f1 series
Korea Central f2 series
Korea Central f8 series
Korea South d1 series
Korea South d11 series
Korea South d14 series
Korea South d15 series
Korea South d16 series
Korea South d3 series
Korea South ds1 series
Korea South ds11 series
Korea South ds12 series
Korea South ds13 series
Korea South ds14 series
Korea South ds15 series
Korea South ds3 series
Korea South e16 series
Korea South e16s series
Korea South e32 series
Korea South e4 series
Korea South e64 series
Korea South e64i series
Korea South e64is series
Korea South e8 series
Korea South f1 series
Korea South f2 series
Korea South f8 series
North Central US d1 series
North Central US d11 series
North Central US d12 series
North Central US d13 series
North Central US d15 series
North Central US d16s series
North Central US d2 series
North Central US d2s series
North Central US d3 series
North Central US d32s series
North Central US d4 series
North Central US d4s series
North Central US d64s series
North Central US d8s series
North Central US ds1 series
North Central US ds11 series
North Central US ds12 series
North Central US ds13 series
North Central US ds14 series
North Central US ds15 series
North Central US ds2 series
North Central US ds3 series
North Central US ds4 series
North Central US e16 series
North Central US e16s series
North Central US e2 series
North Central US e32 series
North Central US e4 series
North Central US e64 series
North Central US e64i series
North Central US e64is series
North Central US e8 series
North Central US f2 series
North Europe d1 series
North Europe d11 series
North Europe d12 series
North Europe d13 series
North Europe d16s series
North Europe d2 series
North Europe d2s series
North Europe d3 series
North Europe d32s series
North Europe d4 series
North Europe d4s series
North Europe d5 series
North Europe d64s series
North Europe d8s series
North Europe ds1 series
North Europe ds11 series
North Europe ds12 series
North Europe ds13 series
North Europe ds14 series
North Europe ds2 series
North Europe ds3 series
North Europe ds4 series
North Europe ds5 series
North Europe e16 series
North Europe e16s series
North Europe e2 series
North Europe e32 series
North Europe e4 series
North Europe e64 series
North Europe e64i series
North Europe e64is series
North Europe e8 series
North Europe f8 series
South Central US d1 series
South Central US d11 series
South Central US d12 series
South Central US d13 series
South Central US d15 series
South Central US d16s series
South Central US d2 series
South Central US d2s series
South Central US d3 series
South Central US d32s series
South Central US d4 series
South Central US d4s series
South Central US d5 series
South Central US d64s series
South Central US d8s series
South Central US ds1 series
South Central US ds11 series
South Central US ds12 series
South Central US ds13 series
South Central US ds14 series
South Central US ds15 series
South Central US ds2 series
South Central US ds3 series
South Central US ds4 series
South Central US ds5 series
South Central US e16 series
South Central US e16s series
South Central US e2 series
South Central US e2s series
South Central US e32 series
South Central US e32s series
South Central US e4 series
South Central US e4s series
South Central US e64 series
South Central US e641 series
South Central US e64is series
South Central US e64s series
South Central US e8 series
South Central US e8s series
South Central US f16 series
South Central US f16 series
South Central US f2 series
South Central US f2 series
South Central US f32 series
South Central US f4 series
South Central US f64 series
South Central US f72 series
South Central US f8 series
South India d1 series
South India d11 series
South India d16 series
Southeast Asia gs4 series
Southeast Asia gs5 series
Southeast Asia m128 series
Southeast Asia m128ms series
Southeast Asia m128s series
Southeast Asia m16ms series
Southeast Asia m32ls series
Southeast Asia m32ms series
Southeast Asia m32ts series
Southeast Asia m64 series
Southeast Asia m64ls series
Southeast Asia m64ms series
Southeast Asia m64s series
Southeast Asia m8ms series
UK South d1 series
UK South d11 series
UK South d12 series
UK South d13 series
UK South d16s series
UK South d2 series
UK South d2s series
UK South d3 series
UK South d32s series
UK South d4 series
UK South d4s series
UK South d64s series
UK South d8s series
UK South ds1 series
UK South ds11 series
UK South ds12 series
UK South ds13 series
UK South ds14 series
UK South ds2 series
UK South ds3 series
UK South ds4 series
UK South e16 series
UK South e16s series
UK South e2 series
UK South e32 series
UK South e4 series
UK South e64 series
UK South e64i series
UK South e64ls series
UK South e8 series
UK South f1 series
UK South f16 series
UK South f8 series
UK South gs4 series
UK South gs5 series
UK South m128 series
UK South m16ms series
UK South m32ls series
UK South m32ms series
UK South m32ts series
UK South m64 series
UK South m64 series
UK South m64s series
UK South m64s series
UK South m8ms series
UK West d1 series
UK West d11 series
UK West d12 series
UK West d13 series
UK West d16s series
UK West d2 series
UK West d2s series
UK West d3 series
UK West d32s series
UK West d4 series
UK West d4s series
UK West d5 series
UK West d64s series
UK West d8s series
UK West ds1 series
UK West ds11 series
UK West ds12 series
UK West ds13 series
UK West ds14 series
UK West ds2 series
UK West ds3 series
UK West ds4 series
UK West ds5 series
UK West e16 series
UK West e16s series
UK West e2 series
UK West e32 series
UK West e4 series
UK West e64 series
UK West e64i series
UK West e64is series
UK West e8 series
UK West f1 series
UK West f16 series
UK West f8 series
UK West m128 series
UK West m128ms series
UK West m128s series
UK West m16ms series
UK West m32ls series
UK West m32ms series
UK West m32ts series
UK West m64 series
UK West m64ls series
UK West m64ms series
UK West m64s series
UK West m8ms series
US Gov Arizona d1 series
US Gov Arizona d11 series
US Gov Arizona d12 series
US Gov Arizona d13 series
US Gov Arizona d14 series
US Gov Arizona d15 series
US Gov Arizona d2 series
US Gov Arizona d3 series
US Gov Arizona d4 series
US Gov Arizona d5 series
US Gov Arizona ds1 series
US Gov Arizona ds11 series
US Gov Arizona ds12 series
US Gov Arizona ds13 series
US Gov Arizona ds14 series
US Gov Arizona ds15 series
US Gov Arizona ds2 series
US Gov Arizona ds3 series
US Gov Arizona ds4 series
US Gov Arizona ds5 series
US Gov Arizona f16 series
US Gov Arizona m128ms series
US Gov Arizona m128s series
US Gov Arizona m16ms series
US Gov Arizona m32ls series
US Gov Arizona m32ms series
US Gov Arizona m32ts series
US Gov Arizona m64ls series
US Gov Arizona m64ms series
US Gov Arizona m64s series
US Gov Arizona m8ms series
US Gov Iowa d1 series
US Gov Iowa d11 series
US Gov Iowa d12 series
US Gov Iowa d13 series
US Gov Iowa d14 series
US Gov Iowa d15 series
US Gov Iowa d2 series
US Gov Iowa d3 series
US Gov Iowa d4 series
US Gov Iowa d5 series
US Gov Iowa f16 series
US Gov Texas d1 series
US Gov Texas d11 series
US Gov Texas d12 series
US Gov Texas d13 series
US Gov Texas d14 series
US Gov Texas d15 series
US Gov Texas d16 series
US Gov Texas d16s series
US Gov Texas d2 series
US Gov Texas d2s series
US Gov Texas d3 series
US Gov Texas d32s series
US Gov Texas d4 series
US Gov Texas d4s series
US Gov Texas d5 series
US Gov Texas d64s series
US Gov Texas d8s series
US Gov Texas ds1 series
US Gov Texas ds11 series
US Gov Texas ds12 series
US Gov Texas ds13 series
US Gov Texas ds14 series
US Gov Texas ds15 series
US Gov Texas ds2 series
US Gov Texas ds3 series
US Gov Texas ds4 series
US Gov Texas ds5 series
US Gov Texas e16 series
US Gov Texas e16s series
US Gov Texas e32 series
US Gov Texas e4 series
US Gov Texas e64 series
US Gov Texas e8 series
US Gov Texas f16 series
US Gov Virginia d1 series
US Gov Virginia d11 series
US Gov Virginia d12 series
US Gov Virginia d13 series
US Gov Virginia d14 series
US Gov Virginia d15 series
US Gov Virginia d2 series
US Gov Virginia d3 series
US Gov Virginia d4 series
US Gov Virginia d5 series
US Gov Virginia ds1 series
US Gov Virginia ds11 series
US Gov Virginia ds12 series
US Gov Virginia ds13 series
US Gov Virginia ds14 series
US Gov Virginia ds15 series
US Gov Virginia ds2 series
US Gov Virginia ds3 series
US Gov Virginia ds4 series
US Gov Virginia ds5 series
US Gov Virginia f16 series
US Gov Virginia gs4 series
US Gov Virginia gs5 series
US Gov Virginia m128 series
US Gov Virginia m128ms series
US Gov Virginia m128s series
US Gov Virginia m10ms series
US Gov Virginia m321s series
US Gov Virginia m32ms series
US Gov Virginia m32ts series
US Gov Virginia m64 series
US Gov Virginia m64ls series
US Gov Virginia m64ms series
US Gov Virginia m64s series
US Gov Virginia m8ms series

**Updated Instances**

West Central US d1 series
West Central US d11 series
West Central US d12 series
West Central US d13 series
West Central US d15 series
West Central US d16 series
West Central US d16s series
West Central US d2 series
West Central US d2s series
West Central US d3 series
West Central US d32s series
West Central US d4 series
West Central US d4s series
West Central US d5 series
West Central US d64s series
West Central US d8s series
West Central US ds1 series
West Central US ds11 series
West Central US ds12 series
West Central US ds13 series
West Central US ds14 series
West Central US ds15 series
West Central US ds2 series
West Central US ds3 series
West Central US ds4 series
West Central US ds5 series
West Central US f16 series
West Central US f2 series
West Europe d1 series
West Europe d11 series
West Europe d12 series
West Europe d13 series
West Europe d2 series
West Europe d3 series
West Europe d4 series
West Europe ds1 series
West Europe ds11 series
West Europe ds12 series
West Europe ds13 series
West Europe ds14 series
West Europe ds2 series
West Europe ds3 series
West Europe ds4 series
West Europe e16 series
West Europe e16s series
West Europe e2 series
West Europe e32 series
West Europe e4 series
West Europe e64 series
West Europe e64i series
West Europe e64is series
West Europe e8 series
West Europe e8 series
West Europe e8 series
West Europe e8 series
West Europe e8 series
West Europe e8 series
West Europe m128 series
West Europe m128ms series
West Europe m128s series
West Europe m16ms series
West Europe m32ls series
West Europe m32ms series
West Europe m32ts series
West Europe m64 series
West Europe m64 series
West Europe m64ls series
<table>
<thead>
<tr>
<th>Region</th>
<th>Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>West Europe</td>
<td>m64ms series</td>
</tr>
<tr>
<td></td>
<td>m64s series</td>
</tr>
<tr>
<td></td>
<td>m8ms series</td>
</tr>
<tr>
<td></td>
<td>d1 series</td>
</tr>
<tr>
<td></td>
<td>d11 series</td>
</tr>
<tr>
<td></td>
<td>d16 series</td>
</tr>
<tr>
<td></td>
<td>ds1 series</td>
</tr>
<tr>
<td></td>
<td>ds11 series</td>
</tr>
<tr>
<td></td>
<td>ds12 series</td>
</tr>
<tr>
<td></td>
<td>ds13 series</td>
</tr>
<tr>
<td></td>
<td>ds14 series</td>
</tr>
<tr>
<td></td>
<td>e64i series</td>
</tr>
<tr>
<td></td>
<td>e64is series</td>
</tr>
<tr>
<td></td>
<td>f4 series</td>
</tr>
<tr>
<td>West India</td>
<td>d1 series</td>
</tr>
<tr>
<td></td>
<td>d11 series</td>
</tr>
<tr>
<td></td>
<td>d12 series</td>
</tr>
<tr>
<td></td>
<td>d13 series</td>
</tr>
<tr>
<td></td>
<td>d15 series</td>
</tr>
<tr>
<td></td>
<td>d16s series</td>
</tr>
<tr>
<td></td>
<td>d2 series</td>
</tr>
<tr>
<td></td>
<td>d2s series</td>
</tr>
<tr>
<td></td>
<td>d3 series</td>
</tr>
<tr>
<td></td>
<td>d32s series</td>
</tr>
<tr>
<td></td>
<td>d4 series</td>
</tr>
<tr>
<td></td>
<td>d4s series</td>
</tr>
<tr>
<td></td>
<td>d64s series</td>
</tr>
<tr>
<td></td>
<td>d8s series</td>
</tr>
<tr>
<td></td>
<td>ds1 series</td>
</tr>
<tr>
<td></td>
<td>ds11 series</td>
</tr>
<tr>
<td></td>
<td>ds12 series</td>
</tr>
<tr>
<td></td>
<td>ds13 series</td>
</tr>
<tr>
<td>West US</td>
<td>d1 series</td>
</tr>
<tr>
<td></td>
<td>d11 series</td>
</tr>
<tr>
<td></td>
<td>d12 series</td>
</tr>
<tr>
<td></td>
<td>d13 series</td>
</tr>
<tr>
<td></td>
<td>d15 series</td>
</tr>
<tr>
<td></td>
<td>d16s series</td>
</tr>
<tr>
<td></td>
<td>d2 series</td>
</tr>
<tr>
<td></td>
<td>d2s series</td>
</tr>
<tr>
<td></td>
<td>d3 series</td>
</tr>
<tr>
<td></td>
<td>d32s series</td>
</tr>
<tr>
<td></td>
<td>d4 series</td>
</tr>
<tr>
<td></td>
<td>d4s series</td>
</tr>
<tr>
<td></td>
<td>d64s series</td>
</tr>
<tr>
<td></td>
<td>d8s series</td>
</tr>
<tr>
<td></td>
<td>ds1 series</td>
</tr>
<tr>
<td></td>
<td>ds11 series</td>
</tr>
<tr>
<td></td>
<td>ds12 series</td>
</tr>
<tr>
<td></td>
<td>ds13 series</td>
</tr>
<tr>
<td></td>
<td>ds14 series</td>
</tr>
<tr>
<td></td>
<td>ds15 series</td>
</tr>
<tr>
<td></td>
<td>ds2 series</td>
</tr>
<tr>
<td></td>
<td>ds3 series</td>
</tr>
<tr>
<td></td>
<td>ds4 series</td>
</tr>
<tr>
<td></td>
<td>e16 series</td>
</tr>
<tr>
<td></td>
<td>e16s series</td>
</tr>
<tr>
<td></td>
<td>e2 series</td>
</tr>
<tr>
<td></td>
<td>e32 series</td>
</tr>
<tr>
<td></td>
<td>e4 series</td>
</tr>
<tr>
<td></td>
<td>e64 series</td>
</tr>
<tr>
<td></td>
<td>e64i series</td>
</tr>
<tr>
<td></td>
<td>e64is series</td>
</tr>
<tr>
<td></td>
<td>e8 series</td>
</tr>
<tr>
<td></td>
<td>f16 series</td>
</tr>
<tr>
<td></td>
<td>gs4 series</td>
</tr>
<tr>
<td></td>
<td>gs5 series</td>
</tr>
<tr>
<td></td>
<td>2 d1 series</td>
</tr>
<tr>
<td></td>
<td>2 d11 series</td>
</tr>
<tr>
<td></td>
<td>2 d12 series</td>
</tr>
<tr>
<td></td>
<td>2 d13 series</td>
</tr>
<tr>
<td></td>
<td>2 d14 series</td>
</tr>
<tr>
<td></td>
<td>2 d15 series</td>
</tr>
<tr>
<td></td>
<td>2 d2 series</td>
</tr>
</tbody>
</table>
West US 2 d3 series
West US 2 d4 series
West US 2 ds1 series
West US 2 ds11 series
West US 2 ds12 series
West US 2 ds13 series
West US 2 ds14 series
West US 2 ds15 series
West US 2 ds2 series
West US 2 ds3 series
West US 2 ds4 series
West US 2 e16 series
West US 2 e16s series
West US 2 e2 series
West US 2 e32 series
West US 2 e4 series
West US 2 e64 series
West US 2 e64i series
West US 2 e64is series
West US 2 e8 series
West US 2 f16 series
West US 2 f2 series
West US 2 f32 series
West US 2 f4 series
West US 2 f64 series
West US 2 f72 series
West US 2 f8 series
West US 2 gs4 series
West US 2 gs5 series
West US 2 m128 series
West US 2 m128ms series
West US 2 m128s series
West US 2 m16ms series
West US 2 m32ls series
West US 2 m32ms series
West US 2 m32ts series
West US 2 m64 series
West US 2 m64ls series
West US 2 m64ms series
West US 2 m64is series
West US 2 m8 series
West US 2 m8ms series

Azure Updates / May 31, 2018

- New Locations
- New Instances
- Updated Instances

New Locations
australia-central02
france-south
australia-central
france-central
New Instances

Australia East e16s series
Australia East e2s series
Australia East e32s series
Australia East e4s series
Australia East e64i series
Australia East e64is series
Australia East e64s series
Australia East e8s series
Australia East m128ms series
Australia East m128s series
Australia East m64ms series
Australia East m64s series
Australia Southeast e16s series
Australia Southeast e2s series
Australia Southeast e32s series
Australia Southeast e4s series
Australia Southeast e64i series
Australia Southeast e64is series
Australia Southeast e64s series
Australia Southeast e8s series
Australia Southeast m128ms series
Australia Southeast m128s series
Australia Southeast m64ms series
Australia Southeast m64s series
Brazil South e16s series
Brazil South e2s series
Brazil South e32s series
Brazil South e4s series
Brazil South e64i series
Brazil South e64is series
Brazil South e64s series
Brazil South e8s series
Canada Central e16s series
Canada Central e2s series
Canada Central e32s series
Canada Central e4s series
Canada Central e64i series
Canada Central e64is series
Canada Central e64s series
Canada Central e8s series
Canada East e16s series
Canada East e2s series
Canada East e32s series
Canada East e4s series
Canada East e64i series
Canada East e64is series
Canada East e64s series
Canada East e8s series
Central India e16s series
Central India e2s series
Central India e32s series
Central India e4s series
Central India e64s series
Central India e8s series
Central US d16s series
Central US d2s series
Central US d32s series
Central US d4s series
Central US d64s series
Central US d8s series
Central US e16s series
Central US e2s series
Central US e32s series
Central US e4s series
Central US e64i series
Central US e64is series
Central US e64s series
Central US e8s series
East Asia e16s series
East Asia e2s series
East Asia e32s series
East Asia e4s series
East Asia e64i series
East Asia e64is series
East Asia e64s series
East Asia e8s series
East US e16s series
East US e2s series
East US e32s series
East US e4s series
East US e64i series
East US e64is series
East US e64s series
East US e8s series
East US 2 e16s series
East US 2 e2s series
East US 2 e32s series
East US 2 e4s series
East US 2 e64i series
East US 2 e64is series
East US 2 e64s series
East US 2 e8s series
East US 2 f16 series
East US 2 f2 series
East US 2 f32 series
East US 2 f4 series
East US 2 f64 series
East US 2 f72 series
East US 2 f8 series
Germany Central e16s series
Germany Central e2s series
Germany Central e32s series
Germany Central e4s series
Germany Central e64i series
Germany Central e64is series
Germany Central e64s series
Germany Central e8s series
Germany Northeast e16s series
Germany Northeast e2s series
Germany Northeast e32s series
Germany Northeast e4s series
Germany Northeast e64i series
Germany Northeast e64is series
Germany Northeast e64s series
Germany Northeast e8s series
Japan East e16s series
Japan East e2s series
Japan East e32s series
Japan East e4s series
Japan East e64i series
Japan East e64is series
Japan East e64s series
Japan East e8s series
Japan East m128ms series
Japan East m128s series
Japan East m64ms series
Japan East m64s series
Japan West e16s series
Japan West e2s series
Japan West e32s series
Japan West e4s series
Japan West e64i series
Japan West e64is series
Japan West e64s series
Japan West e8s series
Japan West m128ms series
Japan West m128s series
Japan West m64ms series
Japan West m64s series
Korea Central e16s series
Korea Central e2s series
Korea Central e32s series
Korea Central e4s series
Korea Central e64i series
Korea Central e64is series
Korea Central e64s series
Korea Central e8s series
Korea South d16s series
Korea South d2s series
Korea South d32s series
Korea South d4s series
Korea South d64s series
Korea South d8s series
Korea South e16s series
Korea South e2s series
Korea South e32s series
Korea South e4s series
Korea South e64i series
Korea South e64is series
Korea South e64s series
Korea South e8s series
North Central US e16s series
North Central US e2s series
North Central US e32s series
North Central US e4s series
North Central US e64i series
North Central US e64is series
North Central US e64s series
North Central US e8s series
North Europe e16s series
North Europe e2s series
North Europe e32s series
North Europe e4s series
North Europe e64i series
North Europe e64is series
North Europe e64s series
North Europe e8s series
South Central US e16s series
South Central US e2s series
South Central US e32s series
South Central US e4s series
South Central US e64i series
South Central US e64is series
South Central US e64s series
South Central US e8s series
South India e16s series
South India e2s series
South India e32s series
South India e4s series
South India e64i series
South India e64is series
South India e64s series
South India e8s series
Southeast Asia e16s series
Southeast Asia e2s series
Southeast Asia e32s series
Southeast Asia e4s series
Southeast Asia e64i series
Southeast Asia e64is series
Southeast Asia e64s series
Southeast Asia e8s series
Southeast Asia m128ms series
Southeast Asia m128s series
Southeast Asia m64ms series
Southeast Asia m64s series
UK South e16s series
UK South e2s series
UK South e32s series
UK South e4s series
UK South e64i series
UK South e64is series
UK South e64s series
UK South e8s series
UK West e16s series
UK West e2s series
UK West e32s series
UK West e4s series
UK West e64i series
UK West e64is series
UK West e64s series
UK West e8s series
US Gov Iowa m128ms series
US Gov Iowa m128s series
Updated Instances

US West 2 f16 series
US West 2 f2 series
US West 2 f32 series
US West 2 f4 series
US West 2 f64 series
US West 2 f72 series
US West 2 f8 series

AWS Updates / May 31, 2018

- New Locations
- New Instances
- Updated Instances

New Locations

EU (Paris)
Asia Pacific (Osaka-Local)

New Instances

US Virginia c5d series
US Oregon c5d series
EU Ireland c5d series
EU Frankfurt c5 series
EU Frankfurt m5 series
EU Frankfurt x1e series
EU Frankfurt c5 series
EU Frankfurt m5 series
EU Frankfurt x1e series
Asia Singapore c5 series
Asia Singapore m5 series
Asia Singapore c5 series
Asia Singapore m5 series
Asia Tokyo c5 series
Asia Tokyo m5 series
Asia Tokyo c5 series
Asia Tokyo m5 series
South America c5 series
South America m5 series
South America c5 series
South America m5 series
US Ohio c5d series
Asia Seoul c5 series
Asia Seoul m5 series
Asia Seoul c5 series
Asia Seoul m5 series
Canada Central c5d series

Updated Instances

US Virginia h1 series
US Oregon h1 series
EU Ireland h1 series
US Ohio h1 series

**Azure Updates / March 22, 2018**

- New Locations
- New Instances

**New Locations**
france-south
france-central

**New Instances**
d16 series - Brazil South
d16 series - Germany Central
d16 series - Germany Northeast
d16 series - Japan East
d16 series - Korea South
d16 series - South India
d16 series - US Gov Texas
d16 series - West Central US
d16s series - Japan East
d16s series - Japan West
d2 series - Brazil South
d2 series - Germany Central
d2 series - Germany Northeast
d2 series - Japan East
d2 series - Korea South
d2 series - South India
d2 series - US Gov Texas
d2 series - West Central US
d2s series - Japan East
d2s series - Japan West
d32 series - Brazil South
d32 series - Germany Central
d32 series - Germany Northeast
d32 series - Japan East
d32 series - Korea South
d32 series - South India
d32 series - US Gov Texas
d32 series - West Central US
d32s series - Japan East
d32s series - Japan West
d4 series - Brazil South
d4 series - Germany Central
d4 series - Germany Northeast
d4 series - Japan East
d4 series - Korea South
d4 series - South India
d4 series - US Gov Texas
d4 series - West Central US
d4s series - Japan East
d4s series - Japan West
d64 series - Brazil South
d64 series - Germany Central
d64 series - Germany Northeast
d64 series - Japan East
d64 series - Korea South
d64 series - South India
d64 series - US Gov Texas
d64 series - West Central US
d64s series - Japan East
d64s series - Japan West
d8 series - Brazil South
d8 series - Germany Central
d8 series - Germany Northeast
d8 series - Japan East
d8 series - Korea South
d8 series - South India
d8 series - US Gov Texas
d8 series - West Central US
d8s series - Japan East
d8s series - Japan West
e16 series - Brazil South
e16 series - Germany Central
e16 series - Germany Northeast
e16 series - Japan East
e16 series - Korea South
e16 series - South India
e16 series - US Gov Texas
e2 series - Brazil South
e2 series - Germany Central
e2 series - Germany Northeast
e2 series - Japan East
e2 series - Korea South
e2 series - South India
e2 series - US Gov Texas
e32 series - Brazil South
e32 series - Germany Central
e32 series - Germany Northeast
e32 series - Japan East
e32 series - Korea South
e32 series - South India
e32 series - US Gov Texas
e4 series - Brazil South
e4 series - Germany Central
e4 series - Germany Northeast
e4 series - Japan East
e4 series - Korea South
e4 series - South India
e4 series - US Gov Texas
e64 series - Brazil South
e64 series - Germany Central
e64 series - Germany Northeast
e64 series - Japan East
e64 series - Korea South
e64 series - South India
e64 series - US Gov Texas
e8 series - Brazil South
e8 series - Germany Central
e8 series - Germany Northeast

FCS-29MARCH2021-UG01    Foundation and CloudScape User Guide
e8 series - Japan East
e8 series - Korea South
e8 series - South India
e8 series - US Gov Texas
h16 series - Central India
h16m series - Central India
h8 series - Central India
h8m series - Central India
m128ms series - UK South
m128s series - UK South
m64ms series - UK South
m64s series - UK South

Azure Updates / March 1, 2018
new instances c5 series AWS - Pacific Sydney
new instances m5 series AWS - Pacific Sydney
new instances c5 series AWS - US Ohio
new instances m5 series AWS - US Ohio
new instances c5 series AWS - Asia Mumbai
new instances m5 series AWS - Asia Mumbai
new instances c5 series AWS - Canada Central
new instances m5 series AWS - Canada Central

Azure Updates / January 22, 2018
new instances c5 series AWS - US California
new instances m5 series AWS - US California
new instances c5 series AWS - EU London
new instances m5 series AWS - EU London
new instance m128ms Microsoft Azure - East US 2
new instances D2-64 v3 series Microsoft Azure - South Central US
new instances E2-E64 v3 series Microsoft Azure - South Central US
new instances M series Microsoft Azure - West Europe
new instances H series Microsoft Azure - Australia East
new instance m128ms Microsoft Azure - West US 2
new instances D2-64 v3 series Microsoft Azure - East Asia
new instances E2-E64 v3 series Microsoft Azure - East Asia
new instances H series Microsoft Azure - Southeast Asia
new instances D2-64 v3 series Microsoft Azure - Japan West
new instances E2-E64 v3 series Microsoft Azure - Japan West
new instances D2-64 v3 series Microsoft Azure - Central India
new instances D2s-64s v3 series Microsoft Azure - Central India
new instances E2-E64 v3 series Microsoft Azure - Central India
new instances D2-64 v3 series Microsoft Azure - UK West
new instances E2-E64 v3 series Microsoft Azure - UK West
new instances H series Microsoft Azure - US Gov Arizona

Azure Updates / December 7, 2017
remove non-current generation instances all AWS regions
new instances c5 series AWS - US Virginia
new instances c5 series AWS - US Oregon
new instances c5 series AWS - EU Ireland
new instances h1 series AWS - US Virginia
new instances h1 series AWS - US Oregon
new instances h1 series AWS - EU Ireland
new instances h1 series AWS - US Ohio
new instances m5 series AWS - US Virginia
new instances m5 series AWS - US Oregon
new instances m5 series AWS - EU Ireland
new instances x1e series AWS - US Virginia
new instances x1e series AWS - US Oregon
new instances x1e series AWS - EU Ireland
new instances x1e series AWS - Asia Tokyo
new instances x1e series AWS - Pacific Sydney

**Azure Updates / November 1, 2017**

add region AWS - Asia Mumbai
new instances x1e.32xlarge AWS - US Virginia
update pricing t2 series AWS - US Virginia
new instances x1e.32xlarge AWS - US Oregon
update pricing t2 series AWS - US Oregon
update pricing t2 series AWS - US California
new instances x1e.32xlarge AWS - EU Ireland
update pricing t2 series AWS - EU Ireland
update pricing t2 series AWS - EU Frankfurt
update pricing t2 series AWS - Asia Singapore
new instances x1e.32xlarge AWS - Asia Tokyo
update pricing t2 series AWS - Asia Tokyo
update pricing t2 series AWS - Pacific Sydney
update pricing t2 series AWS - South America
update pricing t2 series AWS - GovCloud
update pricing t2 series AWS - US Ohio
update pricing t2 series AWS - Asia Seoul
update pricing c4 series AWS - Asia Mumbai
update pricing d2 series AWS - Asia Mumbai
update pricing i2 series AWS - Asia Mumbai
update pricing i3 series AWS - Asia Mumbai
update pricing m4 series AWS - Asia Mumbai
update pricing r3 series AWS - Asia Mumbai
update pricing r4 series AWS - Asia Mumbai
update pricing t2 series AWS - Asia Mumbai
update pricing x1 series AWS - Asia Mumbai
update pricing t2 series AWS - Canada Central
update pricing t2 series AWS - EU London
new instance D1-5 v2 series Microsoft Azure - Central US
new instance D11-15 v2 series Microsoft Azure - Central US
update pricing D2-64 v3 series Microsoft Azure - Central US
update pricing E2-64 v3 series Microsoft Azure - Central US
new instance D2s-64s v3 Microsoft Azure - East US
new instance D1-5 v2 series Microsoft Azure - East US
new instance D11-15 v2 series Microsoft Azure - East US
new instance F v2 series Microsoft Azure - East US
update pricing H series Microsoft Azure - East US
new instance D2s-64s v3 Microsoft Azure - East US 2
new instance D1-5 v2 series Microsoft Azure - East US 2
new instance D11-15 v2 series Microsoft Azure - East US 2
new instance M64s series Microsoft Azure - East US 2
new instance D2-64 v3 Microsoft Azure - North Central US
new instance D1-5 v2 series Microsoft Azure - North Central US
new instance D11-15 v2 series Microsoft Azure - North Central US
new instance E2-64 v3 series Microsoft Azure - North Central US
update pricing H series Microsoft Azure - North Central US
new instance D1-5 v2 series Microsoft Azure - South Central US
new instance D11-15 v2 series Microsoft Azure - South Central US
new instance D2-64 v3 Microsoft Azure - West US
new instance D1-5 v2 series Microsoft Azure - West US
new instance D11-15 v2 series Microsoft Azure - West US
new instance E2-64 v3 series Microsoft Azure - West US
new instance D1-5 v2 series Microsoft Azure - US Gov Iowa
new instance D11-15 v2 series Microsoft Azure - US Gov Iowa
new instance D1-5 v2 series Microsoft Azure - US Gov Virginia
new instance D11-15 v2 series Microsoft Azure - US Gov Virginia
update pricing G series Microsoft Azure - US Gov Virginia
new instance D2-64 v3 Microsoft Azure - North Europe
new instance D1-5 v2 series Microsoft Azure - North Europe
new instance D11-15 v2 series Microsoft Azure - North Europe
new instance E2-64 v3 series Microsoft Azure - North Europe
new instance D2-64 v3 Microsoft Azure - West Europe
new instance D1-5 v2 series Microsoft Azure - West Europe
new instance D11-15 v2 series Microsoft Azure - West Europe
new instance F v2 series Microsoft Azure - West Europe
update pricing H series Microsoft Azure - West Europe
new instance D2-64 v3 Microsoft Azure - Australia East
new instance DS2-64S v3 Microsoft Azure - Australia East
new instance DS1-S5 v2 series Microsoft Azure - Australia East
new instance DS11-S15 v2 series Microsoft Azure - Australia East
new instance E2-64 v3 series Microsoft Azure - Australia East
update pricing G series Microsoft Azure - Australia East
new instance D2-64 v3 Microsoft Azure - Australia Southeast
new instance DS1-S5 v2 series Microsoft Azure - Australia Southeast
new instance DS11-S15 v2 series Microsoft Azure - Australia Southeast
new instance E2-64 v3 series Microsoft Azure - Australia Southeast
new instance DS1-S5 v2 series Microsoft Azure - West Central US
new instance DS11-S15 v2 series Microsoft Azure - West Central US
new instance DS2-64S v3 Microsoft Azure - West US 2
update pricing L series Microsoft Azure - West US 2
new instance DS1-S5 v2 series Microsoft Azure - West US 2
new instance DS11-S15 v2 series Microsoft Azure - West US 2
new instance F v2 series Microsoft Azure - West US 2
new instance M series Microsoft Azure - West US 2
new instance DS1-S5 v2 series Microsoft Azure - East Asia
new instance DS11-S15 v2 series Microsoft Azure - East Asia
new instance DS2-64S v3 Microsoft Azure - Southeast Asia
new instance DS1-S5 v2 series Microsoft Azure - Southeast Asia
new instance DS11-S15 v2 series Microsoft Azure - Southeast Asia
new instance DS1-S5 v2 series Microsoft Azure - Japan East
new instance DS11-S15 v2 series Microsoft Azure - Japan East
update pricing H series Microsoft Azure - Japan East
new instance DS1-S5 v2 series Microsoft Azure - Japan West
new instance DS11-S15 v2 series Microsoft Azure - Japan West
new instance DS1-S5 v2 series Microsoft Azure - Brazil South
new instance DS11-S15 v2 series Microsoft Azure - Brazil South
new instance DS1-S5 v2 series Microsoft Azure - Central India
new instance DS11-S15 v2 series Microsoft Azure - Central India
new instance DS1-S5 v2 series Microsoft Azure - South India
new instance DS11-S5 v2 series Microsoft Azure - South India
new instance D2-64 v3 Microsoft Azure - Canada Central
new instance D1S-5S v2 series Microsoft Azure - Canada Central
new instance DS11-S15 v2 series Microsoft Azure - Canada Central
new instance E2-64 v3 series Microsoft Azure - Canada Central
update pricing G series Microsoft Azure - Canada Central
new instance D2-64 v3 Microsoft Azure - Canada East
new instance D1S-5S v2 series Microsoft Azure - Canada East
new instance DS11-S15 v2 series Microsoft Azure - Canada East
new instance E2-64 v3 series Microsoft Azure - Canada East
new instance DS1-S5 v2 series Microsoft Azure - Germany Central
new instance DS11-S15 v2 series Microsoft Azure - Germany Central
update pricing G series Microsoft Azure - Germany Central
new instance DS1-S5 v2 series Microsoft Azure - Germany Northeast
new instance DS11-S15 v2 series Microsoft Azure - Germany Northeast
new instance D2-64 v3 Microsoft Azure - UK South
new instance D1S-5S v2 series Microsoft Azure - UK South
new instance DS11-S15 v2 series Microsoft Azure - UK South
new instance E2-64 v3 series Microsoft Azure - UK South
update pricing G series Microsoft Azure - UK South
update pricing L series Microsoft Azure - UK South
new instance DS1-S5 v2 series Microsoft Azure - UK West
new instance DS11-S15 v2 series Microsoft Azure - UK West
new instance DS1-S5 v2 series Microsoft Azure - West India
new instance DS11-S15 v2 series Microsoft Azure - West India
new instance D2-64 v3 Microsoft Azure - Korea Central
new instance DS2-64S v3 Microsoft Azure - Korea Central
new instance D1S-5S v2 series Microsoft Azure - Korea Central
new instance DS11-S15 v2 series Microsoft Azure - Korea Central
new instance E2-64 v3 series Microsoft Azure - Korea Central
new instance DS1-S5 v2 series Microsoft Azure - Korea South
new instance DS11-S15 v2 series Microsoft Azure - Korea South

Azure Updates / August 11, 2017

new instances AWS - US Virginia - g3 series
new instances AWS - US Oregon - g3 series
new instances AWS - US California - g3 series
new instances AWS - EU Ireland - g3 series
new instances AWS - GovCloud - g3 series
new instances AWS - US Ohio - g3 series & p2 series
updated pricing AWS - Asia Tokyo - p2 series
updated pricing AWS - Pacific Sydney - p2 series
new instances Azure East US - D-v3 & E-v3 series
new instances Azure East US 2 - D-v3 & E-v3 series
new instances Azure North Central US - H16 instances
new instances Azure South Central US - H16 instances
new instances Azure West US - H16 instances
new instances Azure West US 2 - H series
new instances Azure North Europe - H16 instances
new instances Azure West Europe - H16 instances
new instances Azure Japan East - H16 instances
new instances Azure UK South - H series, G series, & L series
Azure Updates / July 17, 2017
add region AWS - Asia Pacific Seoul

Azure Updates / July 12, 2017
add region AWS - Canada Central
add region AWS - EU London
new instances Azure West Europe - D-v3 & E-v3 series
new instances Azure West US 2 - D-v3, E-v3, G, and L series
new instances Azure Southeast Asia - D-v3 & E-v3 series

Azure Updates / June 8, 2017
update pricing AWS - t2.xlarge (All regions, Windows only)
update pricing AWS - t2.2xlarge (All regions, Windows only)
update pricing AWS US Virginia - m4 series
update pricing AWS US Oregon - m4 series
update pricing AWS US California - m4 series, r4 series
update pricing AWS EU Ireland - m4 series, r4 series
update pricing AWS EU Frankfurt - m4 series, r4 series
update pricing AWS Asia Singapore - m4 series
update pricing AWS Tokyo - m4 series
update pricing AWS Pacific Sydney - m4 series
update pricing AWS South America - m4 series
update pricing AWS Gov Cloud - m4 series, r4 series
update pricing AWS US Ohio - m4 series
update pricing Azure East US - H series
update pricing Azure North Central US - F series, H series
update pricing Azure South Central US - H series
update pricing Azure Australia East - G series
update pricing Azure Brazil South - F series
update pricing Central India - F series
update pricing Azure Canada Central - F series
update pricing Azure Korea Central - F series
new instances Azure East US 2 - M series
new instances Azure West US - L series
new instances Azure North Europe - H series
new instances Australia East - L series
new instances Azure Southeast Asia - G series
new instances Azure Japan East - G series, H series

Azure Updates / May 8, 2017
add region Microsoft Azure - US Gov Virginia
add region Microsoft Azure - East Asia
add region Microsoft Azure - Southeast Asia
add region Microsoft Azure - Japan East
add region Microsoft Azure - Japan West
add region Microsoft Azure - Brazil South
add region Microsoft Azure - Central India
add region Microsoft Azure - West India
add region Microsoft Azure - Germany Northeast
add region Microsoft Azure - Germany Central
add region Microsoft Azure - UK South
add region Microsoft Azure - UK West
add region Microsoft Azure - Korea Central
add region Microsoft Azure – Korea South

**Azure Updates / April 27, 2017**

add provider Oracle Cloud – Compute

**Azure Updates / April 5, 2017**

add region Microsoft Azure – Canada Central
add region Microsoft Azure – Canada East
upgrade i2 → i3 for all AWS Instances

## Subscription Administration

The **Subscription Administration** page (opened by selecting Subscription Administration from the system menu in the top right corner) provides summary information about a subscription, especially around licensing.

Only subscription administrators are able to view subscription details. Users who are not subscription administrators can enter a subscription code to get a list of administrators, who may be contacted to grant administrative privileges.

- **API Key**
- **Subscription Administrators**
- **Licensing**
- **Assessments**

### API Key

The API key is required when accessing the RISC Networks RESTful API. Review RESTful API Access for more information regarding the API. If an API key is not found, the option to generate an API key will be shown.

### Subscription Administrators

A list of subscription administrators who have access to view subscription level information and grant administrative access to other users.

### Licensing

The license count represents the pool available to the subscription. Any licenses attached to a subscription are available for use on any assessments running under that subscription.

- **Continuous License**—This is a license that is available for the life of the subscription. This allows the user to collect performance and dependency data at any time.
- **Flow License**—This license allows the user to collect flow data and understand bandwidth, latency, etc. about connections within the environment.
- **Licensing Burst**—This is a 30 day license of performance and dependency data collection. Once a burst has begun the relevant licensing is available for 30 days from start of the burst.

### Assessments

An assessment represents the sum of data collected by an active appliance (RN150).
What is Max Number of Devices Collecting? This is the maximum number of devices we are collecting at any given time.

Visualize Topology

The Visualize Topology feature draws a layer 2 visualization built from collected network device and interface data.

How the Node-Link Diagram is Constructed

- We create infrastructure nodes from licensed network infrastructure devices such as routers and switches.
- We create edges from the direct connections between these infrastructure nodes. These connections are discovered using CDP.
- We then create parent nodes from the locations to all the devices in those locations

How to Navigate the Diagram

Initially, we restrict the view to only the parent Location nodes to give an overview of the topology of the network. To edit these locations including member their names and member subnets, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To navigate the diagram:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to Add Intelligence &gt; Update Locations.</td>
</tr>
<tr>
<td>2.</td>
<td>Right-click to drill down into a location and reveal its infrastructure nodes.</td>
</tr>
<tr>
<td>3.</td>
<td>(Preview) Right-click an infrastructure device to drill-down to the servers connected to a given node.</td>
</tr>
<tr>
<td>4.</td>
<td>Left-click on a node to focus the view on the direct connections to that node. Other nodes and edges will be grayed-out.</td>
</tr>
<tr>
<td>5.</td>
<td>Left-click on the white space to de-focus the view.</td>
</tr>
</tbody>
</table>

View Options

The “hamburger” menu on the left-hand side of the interface reveals the following options:

“Show” Check Boxes

- IP Address
- Host Name
- Locations—Appends the parent location name to a device name in the display
- Description—The description is pulled from snmp, wmi, or other discovery protocols depending on the source device
- Link Labels—Annotates device-to-device endpoints with the infrastructure interface names

Locations CheckBox List

- All—Shows/hides all nodes and edges in the diagram.
- Locations / Infrastructure Device
• **Checkbox**—Shows/hides the given node and its edges
• **Plus/Minus box**—Expands/contracts the corresponding node

**Export Options**

You can output a given view to two different formats:

• **Export to Visio**—Creates a MS Visio file of the current topology diagram
• **Export to CSV**—Creates a comma-separated-value file of the current node coordinates and node labels

**Total Cost of Ownership**

The Total Cost of Ownership calculator can help determine the cost of creating a on-premise or co-located data center. The calculator considers all physical and virtual servers within an assessment’s scope and determines 5 cost points for each asset:

• **Server Cost** - estimated cost of a comparable server based on processor, cores, and memory metrics
• **Software Cost** - estimated cost of OS software and support (if necessary) to run on the server
• **Facility Cost** - estimated power + miscellaneous rack costs
• **Storage Cost** - estimated cost of storage rack, storage drives, and back-up drives
• **Rack Cost** - estimated cost of rack infrastructure (rack chassis, PDU, TOR switch, etc.)

We use the following metrics for the calculator:

• Processors
• Cores
• Memory (RAM)
• Storage
• OS Distribution
• CPU
Whether a server is determined to be virtual or physical is solely based on our collection methods. For example, if we have WMI access to Windows guests running in a VMware environment, but do NOT have Vsphere access then we will determine those servers to be physical. We recommend enabling every collection type applicable to create the best analysis of an environment.

Table 4-1 • Total Cost of Ownership Calculation

<table>
<thead>
<tr>
<th>Cost</th>
<th>Metrics</th>
<th>Relevant Variables</th>
<th>Cost Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>• Processors</td>
<td>• Timeline in Years</td>
<td>The server cost for physical servers is determined using the following equation:</td>
</tr>
<tr>
<td></td>
<td>• Cores</td>
<td>• Cost of RAM</td>
<td>(Estimated Cost of Server Based On Processors/Cores + Amount of RAM * COST OF</td>
</tr>
<tr>
<td></td>
<td>• Memory in Gb</td>
<td>• Hardware Discount Percentage</td>
<td>RAM) * (1 - HARDWARE DISCOUNT PERCENTAGE) * (1 + HARDWARE MAINTENANCE PERCENTAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hardware Maintenance Percentage Per Year</td>
<td>PER YEAR * TIMELINE IN YEARS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>All virtual servers will have a Server Cost of $0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th>• OS Distribution</th>
<th>• Timeline in Years</th>
<th>• vSphere License Cost</th>
<th>• vSphere Support Cost Percentage Per Year</th>
<th>• Windows License Cost</th>
<th>• Windows Support Cost Percentage Per Year</th>
<th>• RHEL License Cost</th>
<th>• SUSE Physical License Cost</th>
<th>• SUSE Virtual License Cost</th>
<th>• Software Discount Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Software costs are determined using the following decision tree:

- If the device is a VMware Host:
  
  \[ \text{VSPHERE LICENSE COST} \times (1 + \text{TIMELINE IN YEARS} \times \text{VSPHERE SUPPORT COST PERCENTAGE PER YEAR}) \]

- If the device is a physical server running Windows:
  
  \[ \text{WINDOWS LICENSE COST} \times (1 + \text{TIMELINE IN YEARS} \times \text{WINDOWS SUPPORT COST PERCENTAGE PER YEAR}) \]

- If the OS Distribution is Redhat:
  
  \[ \text{RHEL LICENSE COST} \]

- If the OS Distribution is SUSE and the device is a physical server:
  
  \[ \text{SUSE PHYSICAL LICENSE COST} \]

- If the OS Distribution is SUSE and the device is a virtual server:
  
  \[ \text{SUSE VIRTUAL LICENSE COST} \]

All the above costs are discounted by the SOFTWARE DISCOUNT PERCENTAGE variable.
### Table 4-1 • Total Cost of Ownership Calculation

<table>
<thead>
<tr>
<th>Cost</th>
<th>Metrics</th>
<th>Relevant Variables</th>
<th>Cost Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Disk in Gb</td>
<td>Timeline in Years</td>
<td>The storage costs are calculated using the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tb in Storage Rack</td>
<td>- Take ( \text{DISK_IN_GB} / 1024 / \text{TB_IN_STORAGE_RACK} \times \text{TIMELINE_IN_YEARS} \times \text{MONTHS_PER_YEAR} ).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On Premise Monthly Cost of Storage Rack</td>
<td>If hosting on prem, multiply by ( \text{ON_PREMISE_MONTHLY_COST_OF_STORAGE_RACK} ).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Colo Monthly Cost of Storage Rack</td>
<td>Else, multiply by ( \text{COLO_MONTHLY_COST_OF_STORAGE_RACK} ) (Storage Facility cost).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cost of HDD SAN Storage Per Gb</td>
<td>- Then, add ( \text{DISK_IN_GB} \times \text{COST_OF_HDD_SAN_STORAGE_PER_GB} \times (1 - \text{SOFTWARE_DISCOUNT_PERCENTAGE}) \times (1 + \text{STORAGE_SOFTWARE_PERCENTAGE}) ) to the cost (Storage Software cost).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Discount Percentage</td>
<td>- Determine the backup amount in TB by ( \text{DISK_IN_GB} / 1024 \times (1 + \text{SAN_BACKUP_MONTHLY_PERCENTAGE}) \times \text{TIMELINE_IN_YEARS} \times \text{MONTHS_PER_YEAR} ) if \text{ENABLE_INITIAL_BACKUP_SNAPSHOT} ) is true; else just ( \text{DISK_IN_GB} / 1024 \times \text{SAN_BACKUP_MONTHLY_PERCENTAGE} \times \text{TIMELINE_IN_YEARS} \times \text{MONTHS_PER_YEAR} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Storage Software Percentage</td>
<td>- Determine how many TB are processed in a backup window by taking ( \text{MAX_UNCOMPRESSED_SPEED_IN_MB_PER_SEC} \times \text{SECONDS_PER_MINUTE} \times \text{MINUTES_PER_HOUR} / 1024 / 1024 \times \text{BACKUP_WINDOW_IN_HOURS} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAN Backup Monthly Percentage</td>
<td>- Add the cost of tape drives needed cost ( += \text{COST_OF_TAPE_LIBRARY} \times \text{backupAmountInTB} / \text{tbProcessedInBackupWindow} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable Initial Backup Snapshot</td>
<td>- Add the cost of tapes needed cost ( += \text{COST_OF_LTO_TAPE} \times \text{backupAmountInTB} / \text{TAPE_CARTRIDGE_CAPACITY_IN_TB} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max Uncompressed Speed in Mb Per Sec</td>
<td>- Finally, add acquisition cost + discount cost ( += \text{DISK_IN_GB} \times \text{COST_OF_HDD_SAN_STORAGE_PER_GB} \times (1 - \text{SOFTWARE_DISCOUNT_PERCENTAGE}) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup Window in Hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cost of Tape Library</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cost of LTO Tape</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tape Cartridge Capacity in Tb</td>
<td></td>
</tr>
</tbody>
</table>
### Geolocation

This page displays collected public IP address connections to your environment that have been geolocated to their area of origin. This will allow you to understand where your users are located in the world for purposes of cloud migration or to understand where you may be receiving suspicious connections.

This site includes IP2Location LITE data available from [https://lite.ip2location.com](https://lite.ip2location.com).

*Note* • All country codes and names are based on ISO 3166.

---

### Table 4-1 • Total Cost of Ownership Calculation

<table>
<thead>
<tr>
<th>Cost</th>
<th>Metrics</th>
<th>Relevant Variables</th>
<th>Cost Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack</td>
<td>• Rack Chassis Cost</td>
<td></td>
<td>The rack cost for physical servers is determined by taking the total rack cost and uniformly distributing it between all physical servers. Total rack cost is determined using the following equation:</td>
</tr>
<tr>
<td></td>
<td>• PDU Cost Per Rack</td>
<td></td>
<td>(Number of Physical Servers * SERVER UNITS / UNITS IN RACK) * (RACK CHASSIS COST + 2 * PDU COST PER RACK + TOR SWITCHES PER RACK * TOR COST PER RACK) + Number of Physical Servers * RACK DEPLOYMENT COST PER SERVER + Total Server Cost * SPARE SERVER PROVISION PERCENTAGE</td>
</tr>
<tr>
<td></td>
<td>• ToR Switches Per Rack</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ToR Cost Per Rack</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rack Deployment Cost Per Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Spare Server Provision Percentage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Server Units (i.e. Rack Units a server takes up)</td>
<td></td>
<td>All virtual servers will have a rack cost of $0.</td>
</tr>
<tr>
<td></td>
<td>• Units in Rack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility</td>
<td>• Timeline in Years</td>
<td></td>
<td>The facility cost of physical servers is determined using the following equation:</td>
</tr>
<tr>
<td></td>
<td>• Is On Premises</td>
<td></td>
<td>• <strong>On-premise deployment</strong></td>
</tr>
<tr>
<td></td>
<td>• Cost of Kilowatt per Hour</td>
<td></td>
<td>(Estimated power usage from processor count * COST OF KILOWATT PER HOUR * PDU PER RACK * (HOURS PER DAY * DAYS PER YEAR / MONTHS PER YEAR) + ON PREMISE MONTHLY COST OF RACK) * MONTHS PER YEAR * TIMELINE IN YEARS * SERVER UNITS / UNITS IN RACK</td>
</tr>
<tr>
<td></td>
<td>• On Premise Monthly Cost of Rack</td>
<td></td>
<td>• <strong>Co-located deployment</strong></td>
</tr>
<tr>
<td></td>
<td>• Server Units (i.e. Rack Units a server takes up)</td>
<td></td>
<td>(COLO MONTHLY COST OF RACK IN DOLLARS * MONTHS PER YEAR * TIMELINE IN YEARS * SERVER UNITS / UNITS IN RACK)</td>
</tr>
<tr>
<td></td>
<td>• Units in Rack (i.e. Rack Units available in rack)</td>
<td></td>
<td>All virtual servers will have a facility cost of $0.</td>
</tr>
<tr>
<td></td>
<td>• Colo Monthly Cost of Rack in Dollars</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
High Risk Areas

The list of High Risk Areas is sourced primarily from Stanford University. The university compiles its list of high risk countries from a number of sources, including countries that are the subject of Travel Warnings by the U.S. Department of State, and those that are identified as high risk by other U.S. Government sources such as the Department of the Treasury Office of Foreign Assets Control (OFAC), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI). The High Risk Country List also incorporates information from their academic and commercial advisors (e.g., Control Risks). The list is maintained by the Information Security Office, Global Business Services, and the Office of International Affairs and will be updated regularly.

Pin Data

Each pin represents a specific latitude and longitude that one or many IPs have been geolocated to.

On Hover

This will show you how many IPs have been located to that location.

On Click

Clicking will open a detail pane on the right that will have the following panels (from top to bottom):

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Information</td>
<td>This button will pull up a table that contains all connection information we have for that geolocation (e.g. src and dest ports, IPs, protocols, etc.)</td>
</tr>
<tr>
<td>IP Communication</td>
<td>This table shows every internal IP that is communicating with the selected geolocation. The arrow indicates the direction of the communication. The arrow is also relative to the map to make it easier to understand</td>
</tr>
<tr>
<td>Top 3 Protocols</td>
<td>By count of flows (rows in the view connections tables) which protocols were seen most</td>
</tr>
<tr>
<td>Top Threat Level</td>
<td>The Threat Level of devices seen communicating to that location</td>
</tr>
<tr>
<td>Stacks</td>
<td>The application stacks that are communicating to that geolocation</td>
</tr>
<tr>
<td>Locations</td>
<td>The locations that are communicating to that geolocation</td>
</tr>
</tbody>
</table>

Assets & Asset Errors

The Assets page (located underneath Consume Intelligence > Assets) is meant to be the place within the platform where you can understand what assets were discovered in the environment as well as how the environment is changing from an asset perspective. Much of the data on the page is determined by your discoveries. We recommend setting up weekly scheduled discoveries in your environment to track asset changes.

The Assets page has a sub page called Asset Errors which is the main place for troubleshooting as you discover the environment.
Chapter 4  Using the Platform
Reports/Pages

• Assets
• Asset Errors

Assets
You can filter the page by time via the time selector option in the top right. By filtering to a specific range you will only see devices that existed during that range.

Note • If you filter to a time range where only one discovery occurred then the time series graph will change to a bar graph as there is only one data point

Review the How We Collect page to gain a more in-depth understanding of the discovery process/what the appliance is doing.

The Asset page is generated after the RN150 has completed the inventory phase. The appliance/assessment always works in this manner:

• The Asset page lists all devices that responded to an ICMP ping.
• Additionally, if we were able to connect to them using the provided credentials and categorize them, they are further classified into device types (e.g. Windows Server, Windows Workstation, etc).
• Each category in the Asset Report aligns to a specific credential input into the appliance. (i.e. Devices classified as Windows Servers indicate we have WMI access to that box, Generic Server indicates SNMP or SSH accessible devices, Virtual indicates we have vCenter access, etc.).

Asset Errors
This page contains all errors collected in the environment during discovery scans. The errors are organized in two ways, by error or by device. The purpose of this is to allow our user base to quickly troubleshoot by either taking a whole class of errors and ask a sysadmin for resolution or dig into specific error activity on a device. We have included a Resolution field which is our suggested action to be taken to troubleshoot the issue.

Key Takeaway

The report is additive. With each successive rescan of the environment the newly discovered data will be added to that of the previous scan. Data is never removed, even in the event that credentials or subnets are removed or deselected for scanning in the appliance. You can filter to a date to remove anything that is not relevant.

Threats

The Threats page is your hub for understanding how your devices, application stacks, locations, and departments are vulnerable to attacks. We compile and prioritize all vulnerabilities into a single Threat Level rating, but will give you access to all the underlying data so you can determine course of action.

• Threat Levels
• Threat Checks
• High Risk Areas
• Software Vulnerabilities
Threat Levels

Every device who has a Threat Check in your environment will have a Threat Level. The higher the level the greater the security threat of a particular device.

The Threat Level is determined by combining all known vulnerabilities and the behavior of a device.

For example:

- **Level 1**—A device has an unused listening service
- **Level 2**—The above and the device has a vulnerability on an installed package
- **Level 3**—All of the above and that package is running
- **Level 4**—All of the above and that server connects to the internet
- **Level 5**—All of the above and when that server connects to the internet it connects to an anonymous proxy

This example is meant to illustrate the logic behind Threat Levels, not be an exact description of how Threat Level is determined.

We recommend at least investigating every device that’s level 3 and above.

How Are Threats Changing Chart

The chart shows how Threat Levels are changing daily. You can filter this chart and all subsequent tables to specific date ranges either by selecting the start and end dates in the date picker control above the chart or by filtering to a specific date in the tables directly. The page loads with all collected data.

It is important to note that servers will transition between levels based on the time bound nature of certain Threat Checks. For instance, if a server talks to the internet for the first time (when it has not previously) it will trigger a check, but that check will only be relevant for the day we see it exhibit anomalous behavior and then ceases to contribute to the Threat Level.

Threat Checks

Threat Checks are a series of checks that are run nightly on every assessment. Threat Checks contribute to a device’s Threat Level differently depending on their Check Impact. We list the Check Impact classification in the Threat Checks table. Basically, it takes more checks with low impacts to increase Threat Level than checks with High impacts.

<table>
<thead>
<tr>
<th>Check name</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device received connection from high-risk area</td>
<td>High</td>
<td>On day of check, device reported a TCP/IP connection where the IP geolocated to a high-risk area AND was the source of the connection</td>
</tr>
</tbody>
</table>
### Table 4-3 • Threat Checks

<table>
<thead>
<tr>
<th>Check name</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device initiated connection to high-risk area</td>
<td>medium</td>
<td>On day of check, device reported a TCP/IP connection where the IP geolocated to a high-risk area AND was the Destination of the connection.</td>
</tr>
<tr>
<td>Device initiated connection to known anonymous proxy</td>
<td>High</td>
<td>On day of check, device reported a TCP/IP connection where the IP geolocated to a known anonymous proxy where the proxy was the destination of the connection.</td>
</tr>
<tr>
<td>Device received connection from known anonymous proxy</td>
<td>High</td>
<td>On day of check, device reported a TCP/IP connection where the IP geolocated to a known anonymous proxy where the proxy was the source of the connection.</td>
</tr>
<tr>
<td>Device started receiving connections from the Internet</td>
<td>Medium</td>
<td>On day of check, device reported a TCP/IP connection to a public IP address where the public address is the source of the connection AND no public IP address connection as the source was previously reported.</td>
</tr>
<tr>
<td>Device started reaching out to Internet</td>
<td>Low</td>
<td>On day of check, device reported a TCP/IP connection to a public IP address where the public address is the destination of the connection AND no public IP address connection as the destination was previously reported.</td>
</tr>
<tr>
<td>Device receives connections from the Internet</td>
<td>Medium</td>
<td>On day of check, device reported a TCP/IP connection to a public IP address.</td>
</tr>
<tr>
<td>Vulnerable package running</td>
<td>Medium</td>
<td>On day of check, device reported an executable that mapped to an installed package that was found to have a vulnerability.</td>
</tr>
<tr>
<td>Vulnerable package communicating</td>
<td>Medium</td>
<td>On day of check, device reported an executable in its TCP/IP connectivity that mapped to an installed package that was found to have a vulnerability.</td>
</tr>
<tr>
<td>Vulnerable package installed</td>
<td>Low</td>
<td>On day of check, device reported an installed package that was found to have a vulnerability.</td>
</tr>
<tr>
<td>New Listening Process</td>
<td>Low</td>
<td>On day of check, device reported a new listening process that did not exist on the previous day.</td>
</tr>
<tr>
<td>New Installed Software</td>
<td>Low</td>
<td>On day of check, device reported new software installed that did not exist on the previous day.</td>
</tr>
<tr>
<td>New Running Process</td>
<td>Low</td>
<td>On day of check, device reported new process running that did not exist on the previous day.</td>
</tr>
<tr>
<td>Unused Listening Process</td>
<td>Low</td>
<td>On day of check, device reported a listening process to which no connections were observed in the previous 30 days.</td>
</tr>
</tbody>
</table>
High Risk Areas

This panel is meant to show where in the world you may be receiving connections from high risk areas. For a definition of High Risk, see Geolocation.

Software Vulnerabilities

We update our database daily at 4:30AM EST with software vulnerabilities (i.e. Common Vulnerabilities and Exposures (CVEs)) from the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology as well as the Open Vulnerability and Assessment Language (OVAL) repository maintained by the Center for Internet Security. CVE data being used is never more than 24 hrs old.

Our ssh collection pulls rpm/dpkg package lists from Linux servers once per day in the environment and compares the package to those listed in the vulnerability data.

We will pull CVEs for the following Linux distributions:

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debian</td>
<td>8, 9</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>5, 6, 7</td>
</tr>
<tr>
<td>RHEL Server</td>
<td>5, 6, 7</td>
</tr>
<tr>
<td>SLES**</td>
<td>11, 12</td>
</tr>
<tr>
<td>Ubuntu LTS</td>
<td>14.04, 16.04, 18.04</td>
</tr>
<tr>
<td>CentOS</td>
<td>5, 6, 7</td>
</tr>
</tbody>
</table>

No EOL distributions are supported.

Note • CentOS 5 will match against RHEL 5 OVAL but CentOS stopped providing updates in 2017

Note • SLES for SAP Applications is not currently supported, nor are non-LTS versions of Ubuntu.

Threat FAQs

The following are frequently asked questions regarding threats:

- Why do I have so many software vulnerabilities?
- How current is the page?
- Why do I have big dips or spikes in the area chart?
Why do I have so many software vulnerabilities?

A single package can have multiple vulnerabilities, and a single server can have multiple packages, and we look at this every day. It's the multiplicative nature of it.

How current is the page?

It may be up to 48 hours behind from the current time. Since our processing and uploading works on an aggregation method the time between when a particular performance metric is collected to the time it appears in the portal can be up to 48 hours due to post processing.

Why do I have big dips or spikes in the area chart?

Generally, this is caused by performance collection being halted or started on the RN150 appliance. For instance, if you tell the appliance to do a discovery it is not collecting the data needed to do many of the Threat Checks so you would see a corresponding dip in level.

Optimization Scorecard

This report is designed to allow you to easily prioritize your application portfolio for a myriad of optimization activities. As an example, if you use some of the complexity criteria you could understand which apps in your portfolio would be easiest to migrate versus hardest in terms of complexity.

- Standard Templates
- How the Math is Done
- Available Criteria

Standard Templates

This area will contain preloaded criteria, tags, and weights to produce scorecards without the need of the user to complete the scorecard criteria selection process.

Note • More information to come in this section.

How the Math is Done

All criteria start out with a base 100 points available to be granted. The criteria type determines how many points of the base 100 an object receives. The product of this is then multiplied against the weight to determine the final score.
There are two primary types of scoring criteria:

Table 4-5 • Types of Scoring Criteria

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
<th>Description</th>
<th>Final Calculation Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative</td>
<td>Provide a relative scaling score regardless of the assessment size</td>
<td>We will rank all applications from top to bottom based on the selected criteria. The rank number is then divided by the total number of rank-able items to produce a percentile score.</td>
<td>Percentile * 100 * Weight = Score</td>
</tr>
<tr>
<td>Boolean</td>
<td>Provide a scoring mechanism for unrankable or scalable criteria. Boolean means that there is a TRUE/FALSE statement as to whether a given object has the selected criteria.</td>
<td>If a given object (device or stack) has the select criteria (e.g. rscore:rehost) then it will receive 100 points. (Count of Objects w/ selected Criteria) * 100 * Weight = Score</td>
<td></td>
</tr>
</tbody>
</table>

Note • If it is a device level criteria, the stack will receive 100 points for every device that matches the selected criteria.

For more details on the criteria see Available Criteria.

Available Criteria

The following table lists the available criteria.

Table 4-6 • Available Criteria

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Use Case</th>
<th>Type</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictive Cloud Run Cost</td>
<td>Prioritize application stacks with lower cloud cost according to selected Cloud Provider. The source of this pricing can be found on the IaaS Cloud Pricing page</td>
<td>Economical</td>
<td>Relative</td>
<td>Percentile rank all apps by sum of hourly cost</td>
</tr>
<tr>
<td>High Connectivity</td>
<td>Prioritize application stacks with high amounts of connectivity. Connectivity being defined as the number of times we’ve seen this app connecting to any device. This is the opposite of Low Connectivity.</td>
<td>Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by sum netstat connections</td>
</tr>
</tbody>
</table>
### Table 4-6 • Available Criteria

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Use Case</th>
<th>Type</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Connectivity</strong></td>
<td>Prioritize application stacks with low amounts of connectivity. Connectivity being defined as the number of times we've seen this app connecting to any device. This is the opposite of Low Connectivity.</td>
<td>Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by sum netstat connections</td>
</tr>
<tr>
<td><strong>High Number of Users</strong></td>
<td>Prioritize application stacks that connect to many IPs in a chosen location(s). A distinct IP is used to correlate to a user. This is the opposite of Low Number of Users.</td>
<td>Business Impact</td>
<td>Relative</td>
<td>Percentile rank all apps by count of distinct IPs coming from a specific location(s)</td>
</tr>
<tr>
<td><strong>Low Number of Users</strong></td>
<td>Prioritize application stacks that connect to few IPs in a chosen location(s). A distinct IP is used to correlate to a user. This is the opposite of Low Number of Users.</td>
<td>Business Impact</td>
<td>Relative</td>
<td>Percentile rank all apps by count of IPs coming from a specific location(s)</td>
</tr>
<tr>
<td><strong>Location Prioritization</strong></td>
<td>Prioritize application stacks that have more devices located in a specified location(s).</td>
<td>Data Center</td>
<td>Boolean</td>
<td>Devices the chosen location(s) get points</td>
</tr>
<tr>
<td><strong>Devices Over Provisioned</strong></td>
<td>Prioritize application stacks that have more devices that are over provisioned (not using their available resources). This is the opposite of Devices Under Provisioned.</td>
<td>Economical</td>
<td>Relative</td>
<td>This is calculated by pulling all servers in the environment whose 95th percentile CPU or Memory utilization is less than or equal to 50% of their provisioned resources. The CPU and memory percentiles are then added together to form a single utilization metric. This metric is then ranked against the rest of the over provisioned population.</td>
</tr>
</tbody>
</table>
### Table 4-6 Available Criteria

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Use Case</th>
<th>Type</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices Under Provisioned</td>
<td>Prioritize application stacks that have more devices that are under provisioned (exhausting their available resources). This is the opposite of Devices Over Provisioned.</td>
<td>Performance</td>
<td>Relative</td>
<td>This is calculated by pulling all servers in the environment whose 95th percentile CPU or Memory utilization is greater than 50% of their provisioned resources. The CPU and memory percentiles are then added together to form a single utilization metric. This metric is then ranked against the rest of the under provisioned population.</td>
</tr>
<tr>
<td>Low Device Count</td>
<td>Prioritize application stacks that have a low number of devices in them. This is the opposite of High Device Count.</td>
<td>Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by count of servers</td>
</tr>
<tr>
<td>High Device Count</td>
<td>Prioritize application stacks that have a high number of devices in them. This is the opposite of Low Device Count.</td>
<td>Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by count of servers</td>
</tr>
<tr>
<td>Large Storage Footprint</td>
<td>Prioritize application stacks that are using a large amount of storage. This is the opposite of Small Storage Footprint.</td>
<td>Economical &amp; Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by sum of utilized storage</td>
</tr>
<tr>
<td>Small Storage Footprint</td>
<td>Prioritize application stacks that are using a small amount of storage. This is the opposite of Large Storage Footprint.</td>
<td>Speed &amp; Complexity</td>
<td>Relative</td>
<td>Percentile rank all apps by sum of utilized storage</td>
</tr>
<tr>
<td>Stack Tags</td>
<td>Prioritize application stacks that have a specified tag key value pair.</td>
<td>Custom</td>
<td>Boolean</td>
<td>Stacks having the selected key value pair (Tag Key : Tag Value) get points</td>
</tr>
<tr>
<td>Device Tags</td>
<td>Prioritize application stacks that have devices that have a specified tag key value pair.</td>
<td>Custom</td>
<td>Boolean</td>
<td>Stacks having devices having the selected key value pair (Tag Key : Tag Value) get points</td>
</tr>
</tbody>
</table>
Glossary

In this section we have defined many of the key words and definitions found throughout the platform.

- Connectivity Definitions
- Device Type Definitions
- Decommissioned Devices
- Group Definitions
- Licensing Types
- Tags
- IaaS Cloud Pricing

Connectivity Definitions

The following are connectivity definitions.

Table 4-7 • Connectivity Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical vs. Non-Critical</td>
<td>The derivation of Critical vs Non-Critical is primarily driven from the identification of traffic that does NOT play a role in application or supporting system communication. Application process and contexts with corresponding traffic supporting the OS or default system level communication is marked as 'Non-Critical'. Traffic from OS default system processes is also classified as Non-Critical.</td>
</tr>
<tr>
<td>Internal vs. External</td>
<td>An internal connection (displayed as green and blue within the visualization) is one that is internal to the group whereas an external connection (displayed as red and orange within the visualization) is one that is made to a device outside of the select group.</td>
</tr>
<tr>
<td>Application Context</td>
<td>Is a mapped application based on the process that initiated the connection. This proprietary mapping is maintained by RISC Networks.</td>
</tr>
</tbody>
</table>
Device Type Definitions

The following table lists device type definitions.

### Table 4-8 • Device Type Definitions

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Asset Category (2.0)</th>
<th>Device Found During Inventory Collection ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Basic Devices</td>
<td>Via SNMP access AND it reports back as a Wireless Access Point</td>
</tr>
<tr>
<td>ATA</td>
<td>Basic Devices</td>
<td>Via SNMP access AND it reports back as an Analog Telephone Adapter</td>
</tr>
<tr>
<td>Generic SNMP Device</td>
<td>Basic Devices</td>
<td>Via SNMP access though NOT to the required core MIBs</td>
</tr>
<tr>
<td>Printer</td>
<td>Basic Devices</td>
<td>Via SNMP access AND it reports back as a printer</td>
</tr>
<tr>
<td>Telepresence</td>
<td>Basic Devices</td>
<td>Via SNMP access AND it reports back as a Telepresence</td>
</tr>
<tr>
<td>Virtual-Generic SNMP Device</td>
<td>Basic Devices, Virtual Machines</td>
<td>Via VMware access AND we have SNMP access to the device though NOT to the required core MIBs</td>
</tr>
</tbody>
</table>

Note • In the Asset Category (2.0) column, it will be listed in each of the items listed in the column.
Table 4-8 • Device Type Definitions

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Asset Category (2.0)</th>
<th>Device Found During Inventory Collection ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>unknown</td>
<td>Inaccessible Devices</td>
<td>Successfully ping'd the device though NO supported protocols found</td>
</tr>
<tr>
<td>unknownNetworkDevice</td>
<td>Inaccessible Network Infrastructure</td>
<td>With NO protocol access AND UDP port 161 open</td>
</tr>
<tr>
<td>Virtual-unknownNetworkDevice</td>
<td>Inaccessible Network Infrastructure, Virtual Machines</td>
<td>With NO protocol access AND UDP port 161 open (virtual)</td>
</tr>
<tr>
<td>Virtual-Inaccessible Windows Device</td>
<td>Inaccessible Windows, Virtual Machines</td>
<td>Via VMware access only AND port 135 open</td>
</tr>
<tr>
<td>IP-Phone</td>
<td>IP Phones</td>
<td>Via SNMP access AND reports back as an IP Phone</td>
</tr>
<tr>
<td>Generic Server</td>
<td>Linux/UNIX</td>
<td>Via SSH or SNMP access AND reports back as a Linux/UNIX OS</td>
</tr>
<tr>
<td>Virtual-Generic Server</td>
<td>Linux/UNIX, Virtual Machines</td>
<td>Via VMware access AND we have either SSH or SNMP access AND it reports back as a Linux/UNIX OS</td>
</tr>
<tr>
<td>DB NOI</td>
<td>n/a</td>
<td>A derived device that is created to represent a database that was not otherwise inventoried</td>
</tr>
<tr>
<td>NFS</td>
<td>n/a</td>
<td>A derived device (Network File System) that is created if a Generic Server that has a file system mounted from a remote host that cannot be resolved back to a device currently in inventory</td>
</tr>
<tr>
<td>FC Switch</td>
<td>Network Infrastructure</td>
<td>Via SNMP access AND it reports back as a fiber channel switch</td>
</tr>
<tr>
<td>Firewall</td>
<td>Network Infrastructure</td>
<td>Via SNMP access AND it reports back as a Firewall</td>
</tr>
<tr>
<td>l3switch</td>
<td>Network Infrastructure</td>
<td>Via SNMP access AND it reports back as a switch with a routing table</td>
</tr>
<tr>
<td>router</td>
<td>Network Infrastructure</td>
<td>Via SNMP access AND it reports back as a router with a routing table</td>
</tr>
<tr>
<td>switch</td>
<td>Network Infrastructure</td>
<td>Via SNMP access AND it reports back as a switch</td>
</tr>
<tr>
<td>Orphaned - (Device Type)</td>
<td>Virtual Machines</td>
<td>Accessed through VMware AND was licensed but is no longer accessible through VMware</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Virtual Machines</td>
<td>Via VMware access only AND device was not included in subnet range for discovery (ping)</td>
</tr>
</tbody>
</table>
Decommissioned Devices

Devices that are suspected to no longer exist in the IT environment are marked with the RISCdecom flag in the hostname and primary IP address fields. For example, a device with the hostname test-app-01 would be displayed as:

RISCdecom - test-app-01

This flag is applied when a rescan of the environment with the View Inventory Changes feature enabled fails to communicate with a device that was successfully brought into the Asset inventory on a previous scan. Any error received when connecting to the device other than a “permission denied” error will trigger this behavior. The flag can be removed from the device if a subsequent rescan succeeds in communicating with the device.

For instance, if a firewall change results in an inability for the RN150 Virtual Appliance to communicate with a subnet, devices within that subnet will be flagged as RISCdecom when rescanned. A subsequent rescan after correcting the firewall configuration will remove the flag from those devices.

Group Definitions

The following table lists group definitions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSG Groups (aka Infrastructure Service Groups)</td>
<td>Servers in these groups match an existing profile for the particular application group they are placed. Details in table below.</td>
</tr>
</tbody>
</table>
Infrastructure Service Groups

The Intelligent Application Grouping Algorithm identifies and isolates devices which provide infrastructure-critical services. These infrastructure services should not be considered part of any individual Business Service, but rather as a distinct type of IT property which may be evaluated and managed separately from the more business-logic-driven stacks which our algorithm identifies based on common connectivity.

Here is a list of all of the Infrastructure Service Groups we currently create. If any servers in your environment fit into one of these groups, the group will be automatically created and the server will be placed into it, rather than into a Business Service group. Note that for historical reasons, the moniker “RSG” is appended to all Infrastructure Service Groups.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Identification Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>Microsoft Active Directory Domain Controllers</td>
<td>Reported in inventory as PDC or BDC</td>
</tr>
<tr>
<td>Backup Exec Server</td>
<td>Veritas Backup and Recovery service</td>
<td>Running beserver.eve</td>
</tr>
<tr>
<td>BigFix Relay</td>
<td>Endpoint management services</td>
<td>Running besrelay.exe</td>
</tr>
<tr>
<td>BigFix Root</td>
<td>Endpoint management services</td>
<td>Running besrootserver.exe</td>
</tr>
</tbody>
</table>
### Table 4-10 • Infrastructure Service Groups

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Identification Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Service</td>
<td>Certification authority</td>
<td>Running certsrv</td>
</tr>
<tr>
<td>Citrix</td>
<td>Virtual/remote desktop service</td>
<td>Running Citrix ICA Host</td>
</tr>
<tr>
<td>Deep Freeze (NEW)</td>
<td>Image restoration</td>
<td>Running DFServerService.exe</td>
</tr>
<tr>
<td>ECI FMAudit (NEW)</td>
<td>device/printer management</td>
<td>Running Eci FMAudit Onsite</td>
</tr>
<tr>
<td>EG Innovations</td>
<td>Application performance monitoring</td>
<td>Running egurkha and nfping</td>
</tr>
<tr>
<td>EMC Networker</td>
<td>Data protection and backup</td>
<td>Running nrjobd or nsrmmd</td>
</tr>
<tr>
<td>EMC Smarts</td>
<td>Virtual infrastructure management</td>
<td>Running incharge</td>
</tr>
<tr>
<td>Enterprise Vault</td>
<td>Data retention and archiving</td>
<td>Running enterprisevault</td>
</tr>
<tr>
<td>ERA Remote Administrator (NEW)</td>
<td>ERA Remote Administrator</td>
<td>Running eraserver</td>
</tr>
<tr>
<td>ESET Remote Administrator (NEW)</td>
<td>ESET Remote Administrator</td>
<td>Running SET Remote Administrator Service</td>
</tr>
<tr>
<td>Graphite</td>
<td>Graphite monitoring tool</td>
<td>Running carbon-cache or carbon-relay</td>
</tr>
<tr>
<td>Kaspersky Lab Administrator (NEW)</td>
<td>Endpoint security</td>
<td>Running Administrator Kit Server</td>
</tr>
<tr>
<td>Lansweeper (NEW)</td>
<td>IT asset management</td>
<td>Running lansweeperservice</td>
</tr>
<tr>
<td>Lync</td>
<td>Chat (Skype for Business)</td>
<td>Running Lync server processes</td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator</td>
<td>endpoint management</td>
<td>Running ePolicy Orchestrator</td>
</tr>
<tr>
<td>McAfee Foundscan</td>
<td>McAfee antivirus security</td>
<td>Running foundscan</td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td>Mail/calendar/etc</td>
<td>Running Microsoft Exchange Server</td>
</tr>
<tr>
<td>Microsoft Operations Manager</td>
<td>Datacenter monitoring service</td>
<td>Running MonitoringHost.exe</td>
</tr>
<tr>
<td>Nagios</td>
<td>Nagios monitoring tool</td>
<td>Running NRPE daemon</td>
</tr>
<tr>
<td>NAS Devices</td>
<td>Network Storage devices</td>
<td>Hostname matches “netapp” or “isilon”</td>
</tr>
</tbody>
</table>
### Table 4-10 • Infrastructure Service Groups

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Identification Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Devices</td>
<td>Switches, routers, access points</td>
<td>Reported in inventory as switch, router, or access point</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System servers</td>
<td>Running nfsd</td>
</tr>
<tr>
<td>Octopus Deploy Server (NEW)</td>
<td>Continuous delivery and deployment</td>
<td>Running Octopus deploy server process</td>
</tr>
<tr>
<td>Papercut Print Control (NEW)</td>
<td>Printer management</td>
<td>Running pc-server.exe</td>
</tr>
<tr>
<td>Parity Server (NEW)</td>
<td>Endpoint security</td>
<td>Running parityserver.exe</td>
</tr>
<tr>
<td>Quest ChangeAuditor</td>
<td>Monitoring/auditing</td>
<td>Running NPSrvHost.exe</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>Remote desktop</td>
<td>Running rdpshell.exe</td>
</tr>
<tr>
<td>ServiceNow MID Server</td>
<td>Management, Instrumentation, and Discovery service</td>
<td>Running servicenow or mid server application</td>
</tr>
<tr>
<td>ShoreTel IPDS (NEW)</td>
<td>Print Management</td>
<td>Running ShoreTel ipds</td>
</tr>
<tr>
<td>Solarwinds</td>
<td>Solarwinds network monitoring</td>
<td>Running a non-agent solarwind process</td>
</tr>
<tr>
<td>Solarwinds Serv U File Server (NEW)</td>
<td>Managed File Transfer</td>
<td>Running Serv-U.exe</td>
</tr>
<tr>
<td>Sophos (NEW)</td>
<td>Endpoint protection</td>
<td>Running Sophos Management Server or Console</td>
</tr>
<tr>
<td>SOTI Mobicontrol Deployment Server (NEW)</td>
<td>Mobile/IOT endpoint management</td>
<td>Running SOTI mcdeplsvr</td>
</tr>
<tr>
<td>Splunk</td>
<td>data monitoring</td>
<td>Running splunk service processes</td>
</tr>
<tr>
<td>Symantec Endpoint</td>
<td>Symantec antivirus security</td>
<td>Running Symantec Endpoint Protection Manager</td>
</tr>
<tr>
<td>Trend Micro Service</td>
<td>Trend Micro antivirus security</td>
<td>Running Trend Micro or Officescan database server process</td>
</tr>
<tr>
<td>Veeam</td>
<td>Veeam backup and data recovery</td>
<td>Running Veeam.Backup.Service.exe</td>
</tr>
<tr>
<td>VMWare Horizon (NEW)</td>
<td>Virtual desktop manager</td>
<td>Running VMWare Horizon or VMWare View Server processes</td>
</tr>
</tbody>
</table>
Licensing Types

The following are licensing types:

- **Burst**—This is a 30 day license of performance and dependency data collection. Once a burst has begun the relevant licensing is available for 30 days from start of the burst.

- **CCL (Continuous Collection License)**—This is a license that is available for the life of the subscription. This allows the user to collect performance and dependency data at any time.

- **Flow License**—This license allows the user to collect flow data (see the Flow Collection Deployment Guide for more information) and understand bandwidth, latency, etc. about connections within the environment.

Tags

*Note* • The only valid characters for tag keys and values are alphanumeric, comma, period, hyphen, colon, forward slash, space, and underscore. If any other characters are part of a string that would be added programmatically (i.e. in a DNS tag), those characters will be omitted.

The following sections list tags definitions:

- App Stack Level Tags
- Device Level Tags
- Specific Tag Rules
- DNS-Based Tags
- Device State Change Tags
- Performance Profiles

### Table 4-10 • Infrastructure Service Groups

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Service Description</th>
<th>Identification Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Recovery Manager</td>
<td>VMWare disaster recovery</td>
<td>Running vmware-dr</td>
</tr>
<tr>
<td>WSUS</td>
<td>Windows Server Update Service</td>
<td>Running wsusservice.exe</td>
</tr>
<tr>
<td>YumRepo</td>
<td>RedHat repository service</td>
<td>Running yumrepo_sync</td>
</tr>
</tbody>
</table>
App Stack Level Tags

The following table describes App Stack Level tags.

Table 4-11 • App Stack Level Tags

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Owner</td>
<td>The person responsible for an application, this is entered manually.</td>
</tr>
<tr>
<td>Application Description</td>
<td>A description of the application, its purpose, and other relevant metadata. This is entered manually.</td>
</tr>
<tr>
<td>Confirmed By</td>
<td>The user who last successfully selected the Stack Confirmed check box. This is entered automatically and cannot be manually altered.</td>
</tr>
<tr>
<td>Confirmed Date</td>
<td>The timestamp of the last time the stack was confirmed. This is entered automatically and cannot be manually altered.</td>
</tr>
<tr>
<td>Department</td>
<td>The department that owns or is responsible for a particular application stack.</td>
</tr>
<tr>
<td>Saved By</td>
<td>The user who last successfully selected the Stack Saved check box. This is entered automatically and cannot be manually altered.</td>
</tr>
<tr>
<td>Saved Date</td>
<td>The timestamp of the last time the stack was saved. This is entered automatically and cannot be manually altered.</td>
</tr>
<tr>
<td>Stack Confirmed</td>
<td>This is a modal whereby if a stack is confirmed it can signal that the stack has been reviewed for accuracy by the appropriate individuals as well as it becomes unavailable for auto-grouping (aka build app stacks).</td>
</tr>
<tr>
<td>Stack Saved</td>
<td>This is a modal whereby if a stack is saved it can signal that the stack becomes unavailable for auto-grouping (aka build app stacks).</td>
</tr>
</tbody>
</table>

Device Level Tags

The following table lists device level tags.

Table 4-12 • Device Level Tags

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Instance</td>
<td>This is the instance name collected from any identified application running on the host server.</td>
</tr>
<tr>
<td>Database Instance</td>
<td>This is the instance name collected from the database application running on the host server.</td>
</tr>
<tr>
<td>Tier</td>
<td>This is the application tier type that a server matches based on the rules below.</td>
</tr>
</tbody>
</table>
Specific Tag Rules

The following table lists specific tag rules.

<table>
<thead>
<tr>
<th>#</th>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>rscore - Replatform</td>
<td>Server OS Contains 2003 OR Server OS Contains 2000</td>
</tr>
<tr>
<td>2</td>
<td>rscore - Refactor</td>
<td>Server OS Contains SunOS OR Server OS Contains AIX</td>
</tr>
<tr>
<td>3</td>
<td>rscore - Rehost</td>
<td>Server OS Contains 2008 OR Server OS Contains 2012 OR Server OS Contains 2016 OR Server OS Contains 2019</td>
</tr>
<tr>
<td>4</td>
<td>rscore - Rehost</td>
<td>Server OS Contains Red Hat Enterprise Linux 6 OR 7</td>
</tr>
<tr>
<td>5</td>
<td>rscore - Replatform</td>
<td>Server OS Contains Red Hat Enterprise Linux 4 OR 5</td>
</tr>
<tr>
<td>6</td>
<td>rscore - Replatform</td>
<td>Application Runpath Contains mysql OR Application Runpath Contains postgres</td>
</tr>
<tr>
<td>7</td>
<td>rscore - Refactor</td>
<td>Application Runpath Contains oracle</td>
</tr>
<tr>
<td>8</td>
<td>rscore - Refactor</td>
<td>Application Runpath Contains isodx</td>
</tr>
<tr>
<td>9</td>
<td>Tier - Web</td>
<td>Application Runpath Contains httpd OR Application Runpath Contains apache OR Application Context Contains IIS OR Application Runpath Contains nginx</td>
</tr>
<tr>
<td>10</td>
<td>Tier - Middleware</td>
<td>Application Runpath Contains jboss OR Application Runpath Contains tomcat</td>
</tr>
<tr>
<td>11</td>
<td>Tier - Database</td>
<td>Application Runpath Contains mysql OR Application Runpath Contains ora_dba OR Application Runpath Contains postgre OR Application Name Contains SQL</td>
</tr>
</tbody>
</table>

DNS-Based Tags

DNS information is collected from licensed Windows DNS Servers and used to apply tags about A records, CNAME records and other data to device groups. Tags are applied every 24 hours to licensed, inaccessible, and unknown devices, where data is available.

The term Degree is used for DNS-based tags to represent the distance of a CNAME record from an A record. For example, a CNAME record of name.domain.com which directs to a second CNAME record other-name.domain.com before finally directing to an A record of 192.168.56.4 would have a Degree of 2. For definition of DNS-based tags, see below:

- **DNS A Record**—This tag will be applied to a device for any A record that refers to it; A Records have a degree of 0.

---

Table 4-13 • Tag Rules

**Table 4-12 • Device Level Tags**

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rscore</td>
<td>This is the migration pattern that a server matches based on the rules below.</td>
</tr>
</tbody>
</table>
• **DNS CNAME Record - Degree X**—This tag will be applied to a device for any CNAME record that refers to it, where "X" is the degree value. CNAME Records have a degree greater than 0.

• **DNS Entry Point**—This tag will be applied to a device for any DNS records that exist at the largest degree available for that device.
  
  • If a device has only A records (degree 0), all A records would exist in this tag key
  
  • If a device has 5 records at degree 0, 2 at degree 1 and 1 at degree 2, it would have one *Entry Point* tag with the value of the degree 2 record

• **DNS Unique**—This uses the same logic as the *Entry Point* tag, but further filters out any tags that contain the host name of the device.

### Device State Change Tags

The device state change tags indicate the time when, during a scan, the state of a device's accessibility changed. They tag keys are listed and defined below. The tag value is the time of the scan overall, this may vary somewhat from the exact time we attempted to access the device.

**Table 4-14 • Device State Change Tags**

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discovered</td>
<td>This indicates when we first accessed this device.</td>
</tr>
<tr>
<td>stopped responding</td>
<td>This indicates that this device was no longer found. Typically this is a timeout/no response.</td>
</tr>
<tr>
<td>resumed responding</td>
<td>This device did not respond on the previous scan(s), but did on this scan.</td>
</tr>
<tr>
<td>lost authorization</td>
<td>The device responded with an authentication error on this scan.</td>
</tr>
<tr>
<td>regained authorization</td>
<td>The device responded with an authentication error on the previous scan(s), but we were able to successfully authenticate on this scan.</td>
</tr>
</tbody>
</table>

*Note • These tags are only added when there is a change. For instance, if we are unable to authenticate a device for several consecutive scans, a tag would only be applied on the first of those.*
Performance Profiles

We will profile devices based on their performance. These profiles are applied as tags to the device daily as long as we are receiving performance uploads.

Table 4-15 • Performance Profiles

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strained</td>
<td>At least 1 performance issue has been found as calculated across all collected data (i.e. all-time) for the device. This is calculated daily as long as we are receiving performance uploads. Performance issues and their definitions can be found on the Issue Summary Page or by exploring the devices with issues column on the All Applications page.</td>
</tr>
<tr>
<td>In Use</td>
<td>Not determined to fall into the other categories</td>
</tr>
<tr>
<td>Idle</td>
<td>Average CPU and Mem below 20% for the last 90 days of collected data</td>
</tr>
<tr>
<td>Zombie</td>
<td>Average CPU and Mem below 5% AND the device is not the DEST for any known/critical flows</td>
</tr>
</tbody>
</table>

IaaS Cloud Pricing

The following terms relate to IaaS Cloud Pricing:

- **Inventory**—Compares the resources present and usable (provisioned) by the device against the various cloud instances, to provide a match on what is already present in the environment. However, many systems may not be utilizing the full potential of the hardware.

- **Usage**—Determines the instance type that is the best fit for the actual workload (performance) of the system, based on the data collected during the performance collection period of the assessment.

RESTful API Access

RISC Networks RESTful API service provides access to data collected and generated through a RISC Networks engagement. Due to the different format and use cases, the data made available through the API may be grouped differently when compared to the RISC Networks SaaS platform. Access to the API requires the use of an API key. The API key may be requested from the Subscription Administration page by the subscription administrator on the RISC Networks portal. If a code has already been requested, it will be displayed on that page. If you are not the administrator but have the subscription code, you may enter the code on that page to get a list of the administrator(s).

**Documentation**

This is a startup guide. Documentation of the available end points is via swagger-based documentation at:

https://api.riscnetworks.com/docs.html

**Authentication**

The majority of API methods require the use of a temporary authentication token for authentication.

- The token is retrieved through the /1_0/getAuthToken end point.
• Authentication to get the token requires the user id (email address), an assessment code, and an authentication string which incorporates the user’s password and the API key.

• The assessment code can be retrieved via the /1_0/getAssessments end point which authenticates with just the user id and authentication string.

The following steps are required to build the authentication string.

<table>
<thead>
<tr>
<th>Task</th>
<th>To build the authentication string:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Generate an MD5 hash of the user’s password.</td>
</tr>
<tr>
<td>2.</td>
<td>Convert all letters in the string to uppercase.</td>
</tr>
<tr>
<td>3.</td>
<td>Prepend the API key to the hash resulting from Step 2.</td>
</tr>
<tr>
<td>4.</td>
<td>Generate an MD5 hash of the string resulting from Step 3.</td>
</tr>
</tbody>
</table>

**Psuedocode Example**

```plaintext
md5(concat(apiKey, to_upper(md5(password))));
```

The token returned is tied to the user and assessment. It is valid for up to 8 hours, but will expire after 15 minutes of inactivity.

**Example Usage**

You can find a sample client written in Perl [here](#). This example goes through the process of authenticating the user, listing entitled engagements, pulling assets, and pulling stack summary data.
RN150 Migration

Assessment migration is the process of deploying a new RN150 appliance image and moving all of the current assessment info from the existing appliance to the new one.

This section explains the process of migrating an assessment from an existing appliance to a new one.

- **Introduction to RN150 Migration**
- **Migrating to the New RN150**
- **Performing Post-Migration Steps**

**Introduction to RN150 Migration**

Assessment migration is the process of deploying a new appliance and moving all of the current assessment info from an existing appliance to the new one. This process has been designed to be secure, automated, and safe.

- **Purpose of Migration**
- **What You Should Expect**
- **Migration Requirements**
- **Best Practices**

**Purpose of Migration**

In Q4 of 2020, we officially released an new RN150 appliance image based on a new operating system. This was to provide a more secure and maintainable appliance for our customers. The migration process was created to allow customers to transition from existing appliances to the new image. This is highly encouraged as support for the existing appliance will be phased out.

**What You Should Expect**

The basic process is as follows:

1. New appliance is deployed.
2. Get some info from the existing RN150.
3. Enter info in the new RN150.
4. Start the migration on the existing RN150.
5. Wait for migration to complete.
6. Verify continued collection.
Migration Requirements
In order to perform an assessment migration, the following must be in place:

- **Existing appliance**
  - Deployed and running
  - Successfully communicating with the NOC
  - Assessment is running
  - Not currently performing a discovery/inventory scan

- **New appliance**
  - Deployed and running
  - Successfully communicating with the NOC
  - Not provisioned with an assessment

- **IP connectivity**
  - IP connectivity is available from existing appliance to new appliance on port 22
  - If utilizing a FlexDeploy appliance, IP connectivity from the new appliance to the FDP on port 443 is also required

Best Practices
In most deployments, allowances have to be made for the RN150's IP address to have access to devices throughout the network. In order to maintain this, it is first recommended that the new appliance be deployed on the same host/vswitch as the existing appliance. Further, it is recommended that after a successful migration, the existing appliance is shutdown, and the new appliance is configured with its IP address. For most situations, this will result in no changes in the RN150's access for collection.

Given that there is a chance of impacting the ability of the RN150 to connect to devices it needs to collect from, there is a report that will indicate any changes in access pre and post-migration. It is recommended to generate and analyze this report at least a few hours after successful migration to allow time to attempt collection on the environment. For more information, see Generating the Collection Validation Report.
Migrating to the New RN150

This section will guide you through the migration process of the RN150. Deployments of appliances downloaded prior to September 2020 used a CentOS 6 Linux operating system. The migration process will assist in transitioning to the new Debian based appliance image.

The new image can be downloaded by clicking here. Once downloaded, you can go ahead and power it on.

If a proxy is required to access the NOC, it should be configured in the new appliance’s interface settings, as described in Configuring the Virtual Appliances for Proxy Support.

- Configuring Migration on the Existing RN150
- Configure Migration on the New RN150
- Beginning Migration on the Existing RN150
- Back-Out Process

Configuring Migration on the Existing RN150

To configure migration on the existing RN150, perform the following steps.

**Task**

To configure migration on the existing RN150:

1. Browse to the interface of the existing RN150.
2. Enable Advanced Debugging.
3. Click on the Assessment link.

![Image of Configuration Interface](image)
A screen opens stating that your assessment is available.

4. Click **Migrate** next to **Migrate this Assessment to a new Appliance**. A brief explanation of the process will pop up.
5. Click the **Migrate** button. The **Configure Migration** page opens.

![Configure Migration](image)

**Note** • On the **Configure Migration** pages, you will see details for configuring the migration and a section that provides you with the **Encryption Key**. This key is used by the existing RN150 to communicate with the new RN150.

6. Enter the IP address for the new appliance into the **IP Address** field.

7. Click **Submit**. The **Encryption Key** appears on the page.

![Encryption Key](image)

8. Copy the **Encryption Key** to the clipboard. Next, you will need to paste this key into the migration UI of the new appliance.

9. Continue with the steps in **Configure Migration on the New RN150**.
Configure Migration on the New RN150

To configure migration on the new RN150, perform the following steps.

**Task**

**To configure migration on the new RN150:**

1. Browse to the new RN150 Appliance user interface.
2. Accept the EULA if requested and log in. The Please enter one of the following key codes to start bootstrapping page opens.

3. Click the link that says click here to enter the configuration for the migration. The Configure Migration page opens.

4. Enter the IP Address of the existing RN150, and paste the Encryption Key copied from the existing appliance user interface, as described in Configuring Migration on the Existing RN150.

5. Click Submit to apply the configuration.

6. Continue with the steps in Beginning Migration on the Existing RN150.
Beginning Migration on the Existing RN150

To begin migration on the existing RN150, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To begin migration on the existing RN150:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Switch back to the user interface of the existing RN150.</td>
</tr>
<tr>
<td>2.</td>
<td>Click Begin Migration to start the process.</td>
</tr>
</tbody>
</table>

The UI should refresh automatically and redirect to a status page where the migration processes can be monitored.

**Note** • While the migration is in progress, you will not be able to navigate to the rest of the interface of the RN150.

For a more in depth look at each of the statuses, see below:

- **Uninitiated**—This is the default state for an RN150 which is behaving normally. In other words, when the appliance is in this state, no migration is currently active.
- **Data Transferring**—The appliance is in active data transfer / migration to the new appliance.
- **Post Transfer Data**—Once the data has been migrated, the appliance issues a series of jobs to load the data on the new appliance and make required adjustments.
- **New Appliance Activation**—The new appliance has completed the data migration and is now registering the new appliance with the assessment.
- **Migration Complete**—The migration process has successfully completed.
### Back-Out Process

Once the above steps are completed, the remainder of the migration process is fully automated. If there is an error during any of the automated steps, the process to back out the changes depends on the step during which the error occurs.

- If there is an error during any of the following steps, there is an automatic process in place to restore the original state and resume collection on the original RN150:
  - Transferring data to the new RN150
  - Loading the data on the new RN150
  - Performing the local setup on the new RN150
- If an error occurs during one of the above steps, the original RN150 will return to its original dashboard.
- If any of the automated roll-back steps fails, the appliance will be put into an error state and an error message will be shown to the user.
  - This will require a CloudScape engineer to perform roll-back steps to manually restore functionality.
- If there is an error during the wrap-up steps which register the new RN150 after the local setup is complete, manual intervention will be required to roll back the changes.
  - Any error while performing these final steps will result in the appliance moving to an error state and an error message being shown to the user.
  - This will require a CloudScape engineer to perform roll-back steps to manually restore functionality.

### Performing Post-Migration Steps

Once the migration is completed, any subscription administrators and appliance users will receive an email notification of the successful migration. Once this is received, the following optional steps can be performed to ensure data collection can continue uninterrupted.

- Updating the IP Address of the New Appliance
- Generating the Collection Validation Report

#### Updating the IP Address of the New Appliance

To update the IP address of the new appliance, perform the following steps.

<table>
<thead>
<tr>
<th>Task</th>
<th>To update the IP address of the new appliance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Before powering the old appliance off, copy its IP address. This can be found in the URL used to access the appliance.</td>
</tr>
<tr>
<td>2.</td>
<td>Power off the existing appliance, but do not delete it from storage.</td>
</tr>
</tbody>
</table>

**Note** • The existing appliance should be retained in a powered off state until collection has been validated on the new appliance.
3. In the new appliance UI, navigate to the main **Dashboard**, and from there, click on **Interfaces**. The **Interfaces** page opens.

4. On the **Interfaces** page, set the **Method** to **Static** and change the **IP** to the value from the original appliance (that you copied in Step 1).
Generating the Collection Validation Report

In order to confirm that data collection is still working properly on the new appliance, a collection validation report has been provided which checks for devices with collection issues since migration. This report should be generated after migration has been successfully completed and at least one day has passed to allow for data collection to be attempted on all devices.

Task: To generate the Collection Validation Report:

1. Do one of the following:
   - If using the on premises platform, navigate to the IP address of the FlexDeploy.

2. Log in and navigate to Add Intelligence > Available Reports.

3. Click Generate next to the report titled Collection_Validation.online.

After a few minutes, the report will be generated and the Download button will appear.
4. Click **Download** to retrieve the CSV file and open it.

   - If the report is empty, this means that data is being collected from all devices for which collection has been attempted since migration which were being successfully collected from prior to migration.

   - Any devices which appear in this report have had an unsuccessful collection attempt after migration but were being collected from successfully prior to migration.

5. If any devices appear in the report, it is recommended to first check the following:

   - Continued network connectivity between the RN150 and the device including any firewall rules or whitelisting which may need to be updated.

   - Device is still powered on.

   - Any user permissions which may have changed.

6. If the above items are checked and collection is still not able to be validated, please open a support ticket for the Flexera Support team to diagnose the issue.