Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1

March 31, 2016

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Service Provider Segment
Cloud and Network Solutions
Cisco Cloud Architecture for the Microsoft Cloud Platform Solution

Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1

Part: CCAMCP-CNAP-Install1-1.1

CONTENTS

Preface

This document describes the installation of the Cisco Cloud Network Automation Provisioner (CNAP) for the Microsoft Cloud Platform, which includes:

- Installing Cisco CNAP software components
- Installing the Cisco Network Services Orchestrator (NSO) Enabled by Tail-f
- Connecting Cisco CNAP to the Cisco NSO

Document Objective and Scope

This document is part of the Cisco Cloud Architecture for the Microsoft Cloud Platform (CCA MCP) documentation suite for Release 1, summarized in the following table.

Table 2-1 CCA MCP Documentation Suite

Document	Description
Release Notes for Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-RNs/CNAP-Release-Notes.html	Describes caveats and other important information about Release 1.1.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/Foundation/CCAMCP1_Foundation.html	Describes data center infrastructure setup and implementation to support CCA MCP based services.

Table 2-1 CCA MCP Documentation Suite

Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/IaaS_Zinc_Config/CCAMCP1_IaaS_Zinc_Config.html	Describes the Infrastructure as a Service (IaaS) model with per-tenant Cisco CSR 1000V-based router/firewall.
Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Install/CNAP-Install.html	Describes the procedures and initial configuration to install Cisco CNAP in a data center.
Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Admin/CNAP-Admin.html	Describes how the Cisco CNAP Admin Portal is used to create and manage network container plans.
Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Tenant/CNAP-Tenant.html	Describes how the Cisco CNAP Tenant Portal is used to subscribe to network container plans and manage subscriptions.
Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DBSQLaaS/CCAMCP1_DBaaS.html	Describes how Database as a Service (DBaaS) can be deployed over the CCA MCP solution.
Cisco Cloud Architecture for the Microsoft Cloud Platform: DRaaS Application Note, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DRaaS_Application_Note/DRaaS_ASR.html	Describes how Disaster Recovery as a Service (DRaaS) based on Microsoft Azure Site Recovery can be deployed over the CCA MCP architecture.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Backup as a Service Implementation Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/BaaS/BaaS_CommVault.html	Describes how Backup as a Service (BaaS) based on Commvault Simpana software can be deployed over the CCA MCP architecture.

This document only describes the installation of Cisco CNAP software. For information on using the Cisco CNAP Admin and Tenant Portals, see the Admin and Tenant Portal guides listed in the table above.

Useful Product Documentation

- Cisco Adaptive Security Appliance 5585 (Cisco ASA 5585)
  http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html
- Cisco Aggregation Services Router—Cisco ASR 9000 and Cisco ASR 1000
  - Cisco ASR 9000
    http://www.cisco.com/c/en/us/products/routers/asr-9000-series-aggregation-services-routers/index.html
  - Cisco ASR 1000
    http://www.cisco.com/c/en/us/products/routers/asr-1000-series-aggregation-services-routers/index.html
- Cisco Application Centric Infrastructure (Cisco ACI)
  http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html
- Cisco Application Policy Infrastructure Controller (Cisco APIC)
  http://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html
- Cisco Cloud Services Router 1000V (Cisco CSR 1000V)
  http://www.cisco.com/c/en/us/products/routers/cloud-services-router-1000v-series/index.html
- Cisco Network Services Orchestrator (Cisco NSO)
  http://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
- Cisco Nexus 9000
  http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html
- Citrix NetScaler VPX
  https://www.citrix.com/products/netscaler-application-delivery-controller/platforms.html

Installing Cisco Cloud Network Automation Provisioner

Introduction

The Cisco Cloud Architecture for Microsoft Cloud Platform (CCA for MCP) solution delivers IaaS, PaaS, and SaaS with integrated management software. The data center infrastructure is built with Cisco Application Centric Infrastructure (ACI) for the Data Center Fabric and Cisco UCS-based compute, Cisco Adaptive Security Appliance (ASA) firewall for security, and Cisco Aggregation Services Routers (Cisco ASR 9000 and Cisco ASR1000) data center edge routers. Additionally, Cisco virtualized network functions such as Cisco Cloud Services Router 1000V (CSR 1000V) are used to implement tenant services.

Microsoft Hyper-V Hypervisor is used as the virtualizing layer for compute to run tenant workloads. The Management Stack is based on Microsoft Windows Azure Pack (WAP), which allows service providers to create plans and tenant administrators to subscribe to those plans.

CCA for MCP enables service providers to host and offer sophisticated tenant network containers over a Cisco cloud infrastructure, enabling tenants to deploy multi-tier applications in the cloud. The provisioning of such containers is enabled by the use of the Cisco Advance Data Center Network Resource Provider in the Microsoft Windows Azure Pack Portals. Cisco Cloud Network Automation Provisioner (CNAP) software includes the Cisco Advance Data Center Resource Provider component, which exposes the Cisco infrastructure resources to the:

- Service Provider Cloud Admin to publish plans that offer complex network containers
- Tenant to use the subscriptions to instantiate the network containers and, using the VMClouds Resource Provider, deploy tenant workloads and attach to tenant Virtual networks

A Microsoft WAP administrator can use Cisco CNAP for MCP Admin Portal to configure, manage, and administer Cisco Data Center Network resources. Cisco CNAP provides the capability to create tenant containers with sophisticated network services such as tenant edge routing, multiple security zones, firewalling, NAT, MPLS VPN access, and Server Load Balancing. The administrator uses the portal to define and set up the available plans that will be visible in the Tenant Portal and that can be consumed by tenants. Tenants consume resources by using the Tenant Portal to subscribe to an available plan. This allows service providers to offer differentiated plans that provide more value to tenants and generate more revenue for service providers, with the convenience of automation to deploy sophisticated containers for tenants.

For more information, see: http://www.cisco.com/go/cloud.

Prerequisites for Installing Cisco Cloud Network Automation Provisioner

Note Cisco's commitment to security requires that the target system(s) on which the Cisco CNAP Software is installed must be up to date with all known security patches for the Microsoft Window Server Operating System, Microsoft .NET Framework, Microsoft ASP.NET, Microsoft SQL Server, and Windows Azure Pack.
Administrators can consider using the Microsoft Baseline Security Analyzer (MBSA) scan tool to identify common security misconfigurations and missing security updates on system endpoints: https://technet.microsoft.com/en-us/security/cc184924.aspx

Before you install Cisco CNAP, you **must**:

- Set up and configure network resources and services.
- Install and configure Microsoft Windows Azure Pack.
- Install and configure Cisco Application Centric Infrastructure plugins for Microsoft System Center Virtual Machine Manager and Hyper-V.
- Set up the environment and target virtual machines.
- Install and configure Microsoft Service Bus 1.1.
- Add the VMM Service into a Local Trust with the Cisco CNAP Admin API server.

Caution Every time you install Cisco CNAP, the database is recreated. To preserve your data, you should always backup your database before reinstalling Cisco CNAP.

Setting Up and Configuring Network Resources and Services

Before you install Cisco CNAP, you should:

- Build the data center infrastructure—Refer to the *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* for detailed information on building data centers using physical components to implement compute, storage, and data center networking to create a pool of resources that are then used to offer services to tenants.
- Configure specific services—The services that are supported by the Cisco Cloud Architecture for the Microsoft Cloud Platform architecture include Infrastructure as a Service (IaaS) with Zinc Container, Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc. You must set up these services before you use Cisco CNAP to configure access to them. See Table 2-1 in the Preface for:
  - Specific configuration requirements for these services in the various configuration documents.
  - More information on using Cisco CNAP to configure access to these services, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 1.1*.

Installing and Configuring Microsoft Windows Azure Pack

Microsoft WAP must be installed before installing Cisco CNAP. This document does not discuss the installation of Microsoft WAP. The basic prerequisites for Microsoft WAP are:

- Windows Server 2012 R2 and Patches
- Microsoft SQL Server
- System Center 2012 R2

For comprehensive information on Microsoft WAP prerequisites and installation, see:

- Windows Azure Pack for Windows Server
  https://technet.microsoft.com/en-us/library/dn296435.aspx

In particular, see:

- Windows Azure Pack installation checklist
  https://technet.microsoft.com/en-us/library/dn469338.aspx
- Windows Azure Pack system requirements overview
  https://technet.microsoft.com/en-us/library/dn296442.aspx

Useful Microsoft Windows Azure Pack References

The following sources may provide useful information about Microsoft WAP:

- WAP Wiki—Source for general information on Microsoft WAP
  http://social.technet.microsoft.com/wiki/contents/articles/20689.the-azure-pack-wiki-wapack.aspx
- Building Clouds Blog—Maintained by the Windows Server & System Center Customer Advisory Team.
  - Overview of WAP on the blog
    http://blogs.technet.com/b/privatecloud/archive/2013/12/20/building-clouds-windows-azure-pack-blog-post-overview.aspx
  - Installing and Configuring Series
    http://blogs.technet.com/b/privatecloud/archive/2013/12/06/windows-azure-pack-installing-amp-configuring-series.aspx
  - Troubleshooting Installation and Configuration of WAP—Introduction
    http://blogs.technet.com/b/privatecloud/archive/2013/11/05/troubleshooting-configuration-of-windows-azure-pack.aspx
- PLA—Important as the IaaS Fabric and Fabric Management PLAs are the root source for SPRA and Fast Track.
  - Overview
    http://blogs.technet.com/b/privatecloud/archive/2014/04/28/iaas-product-line-architecture-available-for-download.aspx
  - Deployment Guide
    https://gallery.technet.microsoft.com/Infrastructure-as-a-ecf1cc0b
  - Cisco Fast Track—Provides extensive step-by-step instructions
    http://www.cisco.com/c/en/us/solutions/data-center-virtualization/microsoft-applications-on-cisco-ucs/index.html

Installing and Configuring Cisco Application Centric Infrastructure Plugins for Microsoft System Center Virtual Machine Manager and Hyper-V

To enable the Microsoft System Center Virtual Machine Manager (SCVMM) to communicate with the Cisco Application Policy Infrastructure Controller (APIC), every host in your Hyper-V cluster must run the Hyper-V plugin and you also must install the SCVMM plugin. Do not use the Cisco Application Centric Infrastructure (ACI) Resource Provider for WAP.

Cisco ACI is a next-generation data center fabric infrastructure designed using an application policy model, allowing the entire data center infrastructure to better align with application delivery requirements and business policies of an organization. Integrating with Microsoft Windows-based application servers running the Microsoft Hyper-V hypervisor, Cisco ACI provides tight integration between physical and virtual application environments.

Cisco extends the Cisco ACI policy framework to the Microsoft Windows Server Hyper-V with Microsoft System Center and Microsoft Azure Pack.

Integrating Cisco Application Centric Infrastructure with Microsoft Hyper-V

The Cisco APIC integrates with a SCVMM instance to transparently extend the Cisco ACI policy framework to Microsoft Hyper-V workloads. The Cisco APIC uses Application Network Profiles (ANPs) to represent the Cisco ACI policy. The ANPs model the logical representation of all components of the application and its interdependencies on the Cisco ACI fabric. After these ANPs are defined in the Cisco APIC, the integration between Microsoft SCVMM and the Cisco APIC helps ensure that these network policies can be applied to Microsoft Hyper-V workloads. The network policies and logical topologies (VLANs, subnets, etc.) that have traditionally-dictated application designs are now applied based on the ANP through the Microsoft APIC.

The Cisco ACI service plugin helps enable management of network infrastructure through the APIC REST API. The Cisco APIC integrates with Microsoft SCVMM to simplify workload connectivity. To connect Windows Server Hyper-V workloads to the Cisco ACI fabric, the virtualization administrator simply needs to associate the virtual machines with the virtual machine networks created by the Cisco APIC that appear under the logical switch in Hyper-V.

The following summarizes the steps involved:

- Install the APIC SCVMM Agent on SCVMM.
- Configure APIC IP Settings with APIC credentials on the SCVMM Agent.
- Generate the APIC Hyper-V Agent OpFlex certificate.
- Add the OpFlex certificate policy to APIC.
- Install the APIC Hyper-V Agent on the Hyper-V server.
- Verify the APIC SCVMM Agent installation on SCVMM.
- Verify the APIC Hyper-V Agent installation on the Hyper-V server.
- Create SCVMM Domain Profiles.
- Verify the SCVMM VMM Domain and SCVMM VMM.
- Deploy the logical switch to the host on SCVMM.

For more information, see:

- Cisco Application Centric Infrastructure and Microsoft SCVMM and Azure Pack
  http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-732080.html

- Cisco ACI with Microsoft SCVMM
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/virtualization/b_ACI_Virtualization_Guide/cisco____aci___with_microsoft_scvmm.html
- Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0
http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/Foundation/CCAMCP1_Foundation.html

Setting Up the Environment and Target Virtual Machines

For information on setting up the environment for Microsoft WAP including specific guidelines on allocating virtual machines (VMs), refer to:

- Microsoft Service Provider Reference Architecture:
    - SPRA Foundation—Converged Infrastructure
    http://download.microsoft.com/download/9/7/B/97BC02C7-3E93-4DBE-BE31-CA7E6C80B05E/SPRA v2 1 - MT - Foundation - Converged Infrastructure.docx
    - Service Provider Reference Architecture—Desktop Hosting Using RDSH
    http://download.microsoft.com/download/A/3/0/A30480C9-86D3-4535-96D8-2BEEB1DA9E1D/Service Provider Reference Architecture - Desktop Hosting using RDSH.docx
    - Service Provider Reference Architecture—Database Hosting Using SQL 2014
    http://download.microsoft.com/download/0/8/A/08AC4D77-C66B-4749-89AD-6AC74E79B59B/Service Provider Reference Architecture - Database Hosting using SQL Server 2014.docx
- FlexPod Datacenter with Microsoft Private Cloud Fast Track 4.0 and Cisco Nexus 9000 Series Switches Design Guide
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_mspc40_c-mode_n9k_design.html
- FlexPod Datacenter with Microsoft Private Cloud Fast Track 4.0 and Cisco Nexus 9000 Series Switches Deployment Guide
https://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m-spc40_cmode_n9k.pdf

Note Cisco CNAP software is installed on the Admin Portal server, Tenant Portal server, and CNAP Backend server. CNAP Backend can be installed on the Admin API server.

Installing and Configuring Microsoft Service Bus 1.1

During or after WAP installation, you must install and configure Microsoft Service Bus 1.1, which is not installed during a default WAP installation.

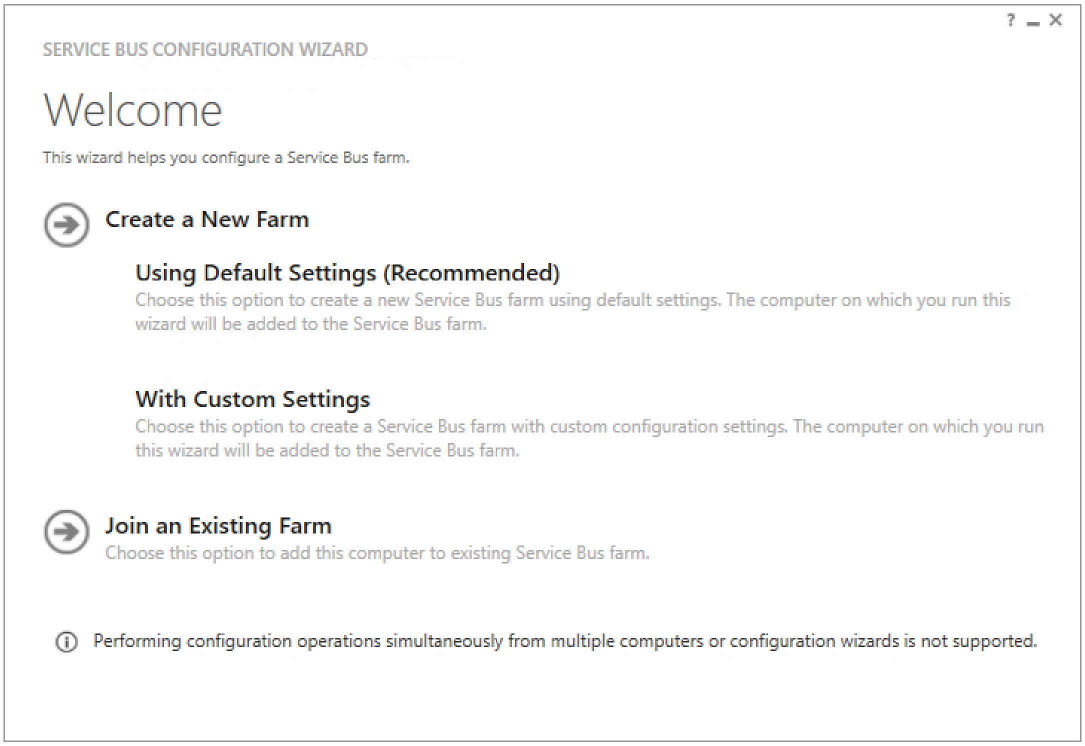
Note Microsoft Service Bus 1.1 should be installed on the Admin API server.

The Microsoft Service Bus 1.1 can be downloaded using the Microsoft Web Platform Installer and can be found in the same location as all the other WAP components.

Step 1 Run the Service Bus Configurator.

You see the following screen.

Figure 1-1 Service Bus Configuration Wizard



SERVICE BUS CONFIGURATION WIZARD

Welcome

This wizard helps you configure a Service Bus farm.

Create a New Farm

Using Default Settings (Recommended)
Choose this option to create a new Service Bus farm using default settings. The computer on which you run this wizard will be added to the Service Bus farm.

With Custom Settings
Choose this option to create a Service Bus farm with custom configuration settings. The computer on which you run this wizard will be added to the Service Bus farm.

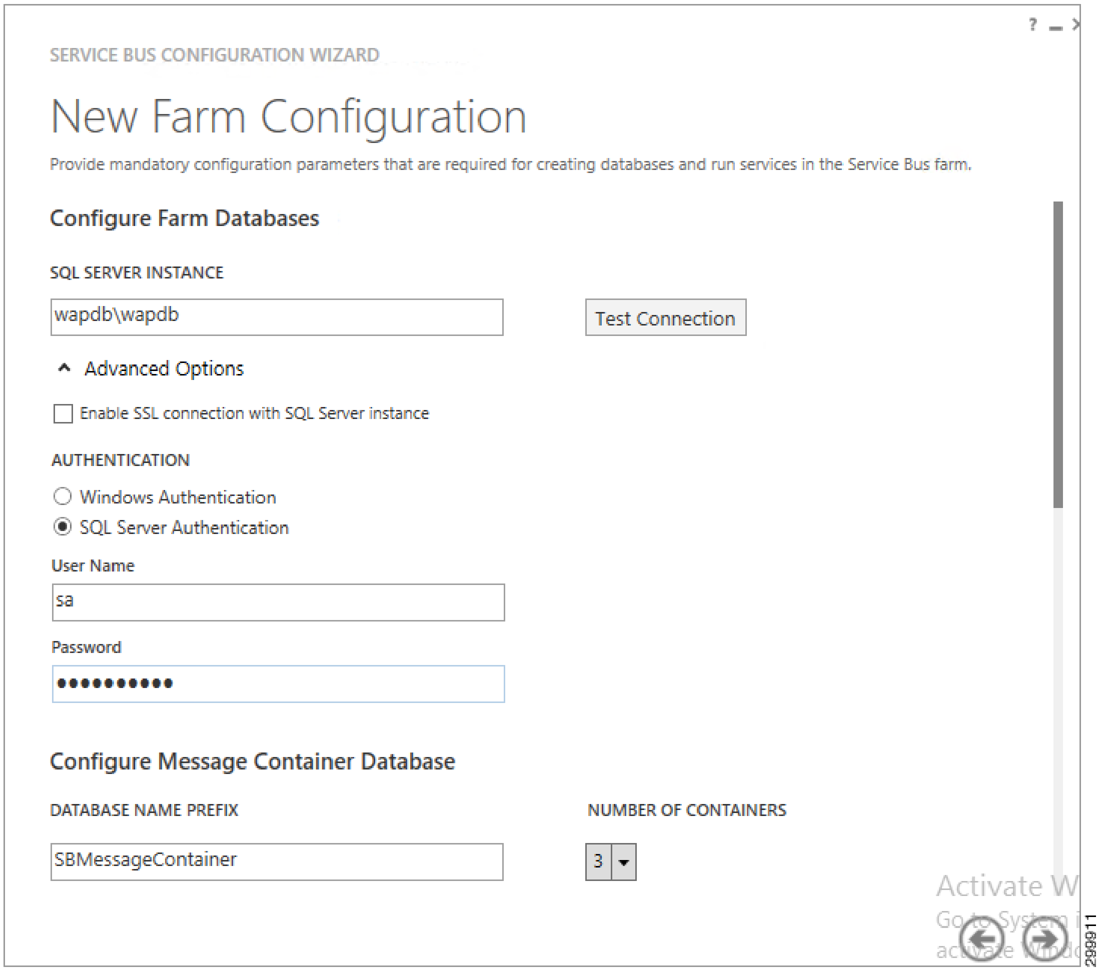
Join an Existing Farm
Choose this option to add this computer to existing Service Bus farm.

Performing configuration operations simultaneously from multiple computers or configuration wizards is not supported.

Step 2 Select **Create New Farm –> Using Default Settings (Recommended)**.

You see the following screen.

Figure 1-2 New Farm Configuration—1 of 2



SERVICE BUS CONFIGURATION WIZARD

New Farm Configuration

Provide mandatory configuration parameters that are required for creating databases and run services in the Service Bus farm.

Configure Farm Databases

SQL SERVER INSTANCE: wapdb\wapdb

Advanced Options

□ Enable SSL connection with SQL Server instance

AUTHENTICATION

○ Windows Authentication
● SQL Server Authentication

User Name: sa

Password: ●●●●●●●●●●

Configure Message Container Database

DATABASE NAME PREFIX: SBMessageContainer

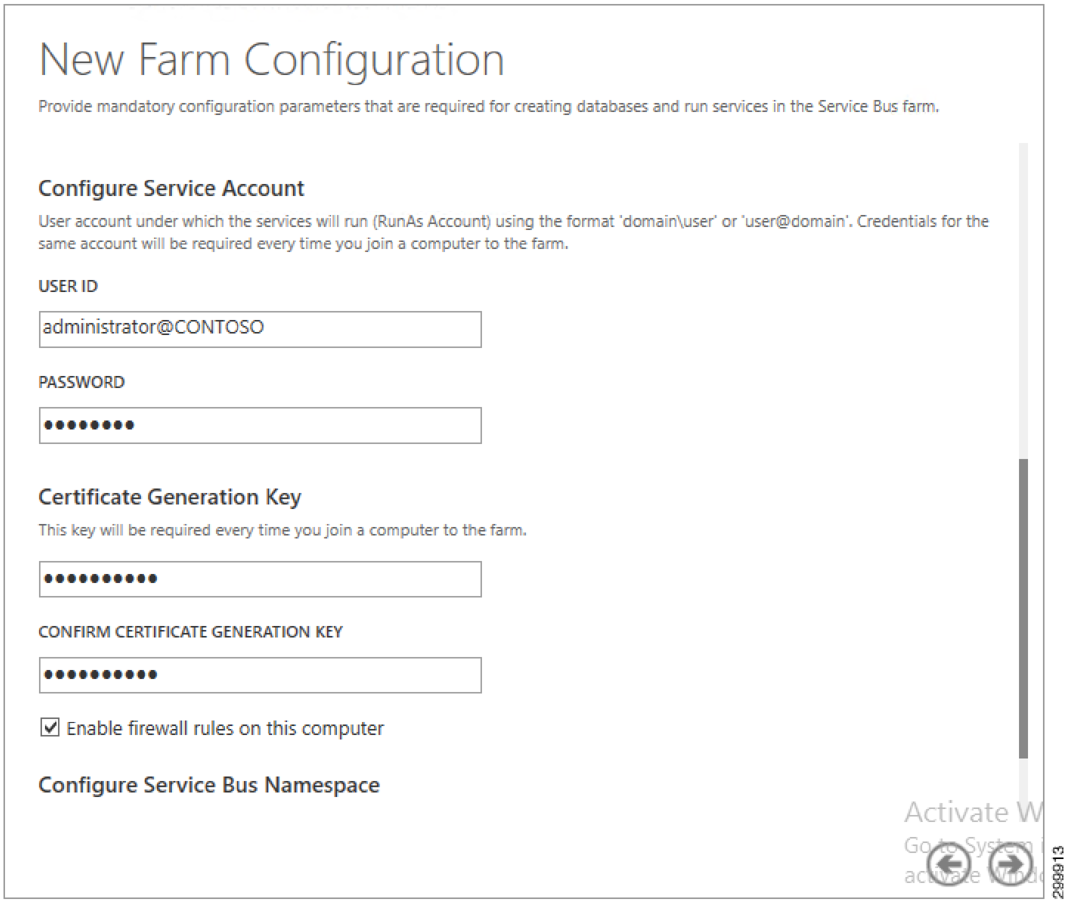
NUMBER OF CONTAINERS: 3

Step 3 In the **SQL Server Instance** field, enter your WAP DB Instance.

Step 4 Select **Advanced Options** and select either **Windows Authentication** or **SQL Server Authentication**.

Step 5 Scroll down so you see the following screen.

Figure 1-3 *New Farm Configuration—2 of 2*



New Farm Configuration

Provide mandatory configuration parameters that are required for creating databases and run services in the Service Bus farm.

Configure Service Account

User account under which the services will run (RunAs Account) using the format 'domain\user' or 'user@domain'. Credentials for the same account will be required every time you join a computer to the farm.

USER ID

administrator@CONTOSO

PASSWORD

••••••••

Certificate Generation Key

This key will be required every time you join a computer to the farm.

••••••••••

CONFIRM CERTIFICATE GENERATION KEY

••••••••••

☑ Enable firewall rules on this computer

Configure Service Bus Namespace

Step 6 Enter a Password and the Certificate Generation Key (and confirm the key).

Step 7 Click the right arrow (–>) and click **Okay**.

Cisco CNAP will configure the proper Service Bus Name Space (SBNameSpace) when it is installed.

Adding the VMM Service into a Local Trust with the Cisco CNAP Admin API Server

The VMM Service needs to be added into a local trust with the Cisco CNAP Admin API server. The VMM Service can be the SCVMM host or the VMM Cluster role if configured.

For example:

```
winrm set winrm/config/client @{TrustedHosts="IP/Hostname of VMM Service"}
```

Overview of Cisco Cloud Network Automation Provisioner Installation

This section describes the installation and initial setup of the Cisco CNAP, which includes:

- Installing the Cisco Cloud Network Automation Provisioner
- Installing the Cisco NSO
- Connecting Cisco CNAP to the Cisco NSO

Post-installation verification procedures are also outlined.

Cisco Cloud Network Automation Provisioner Software Components and Prerequisites

Table 1-1 lists the Cisco CNAP components and prerequisites. This document only describes the installation of the Cisco CNAP Admin Portal, Tenant Portal, and Backend Service.

Note Cisco CNAP software is installed on the Admin Portal server, Tenant Portal server, and CNAP Backend server. CNAP Backend can be installed on the Admin API server.

Note The basic prerequisites for Microsoft WAP are:
-Windows Server 2012 R2 and Patches
-Microsoft SQL Server
-System Center 2012 R2
For more information, see Installing and Configuring Microsoft Windows Azure Pack.

Table 1-1 ??Cisco CNAP Components and Prerequisites??

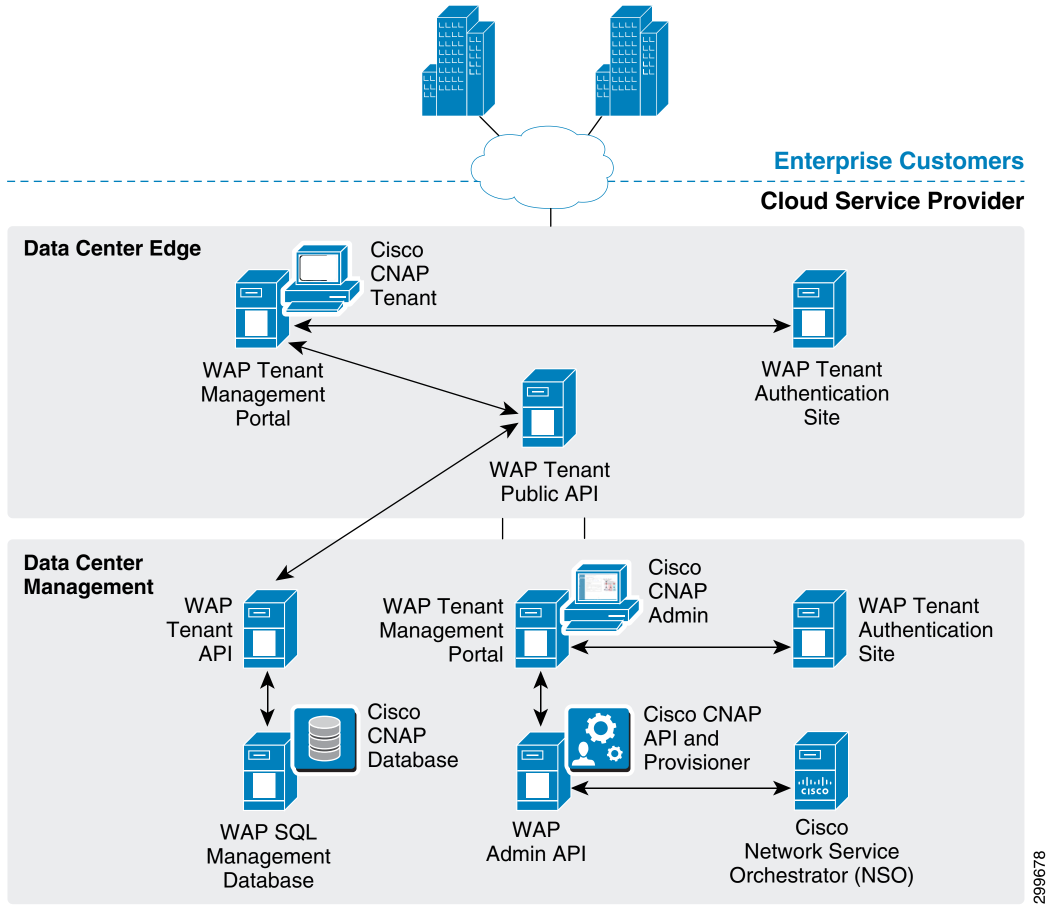
Component	Description	Prerequisites
Cisco CNAP Admin	Cisco CNAP WAP Admin Portal Extension	Microsoft WAP: Admin Site Microsoft WAP: Admin API Microsoft WAP: Prerequisites
Cisco CNAP Tenant	Cisco CNAP WAP Tenant Portal Extension	Microsoft WAP: Tenant Site Microsoft WAP: Tenant Public API Microsoft WAP: Prerequisites
Cisco CNAP API and Provisioner	Cisco CNAP Backend: RP REST API Data Center Provisioner	Microsoft WAP: Admin API Microsoft WAP: Prerequisites Service Bus 1.1 for Windows Server (do not integrate with Microsoft WAP) Microsoft Service Provider Foundation (URL and Service Account)

Table 1-1 ??Cisco CNAP Components and Prerequisites??

Cisco CNAP Database	Cisco CNAP Database	Microsoft SQL Server: Versions supported in a Microsoft WAP deployment
Cisco Network Service Orchestrator (NSO)	Cisco Network Services Orchestrator (NSO) Enabled by Tail-f	RHEL Server/CentOS Server 6.5-7 Java JDK 1.8.45+

Figure 1-4 shows the interrelationships of the various components.

Figure 1-4 Cisco CNAP Components



Installing the Cisco Cloud Network Automation Provisioner

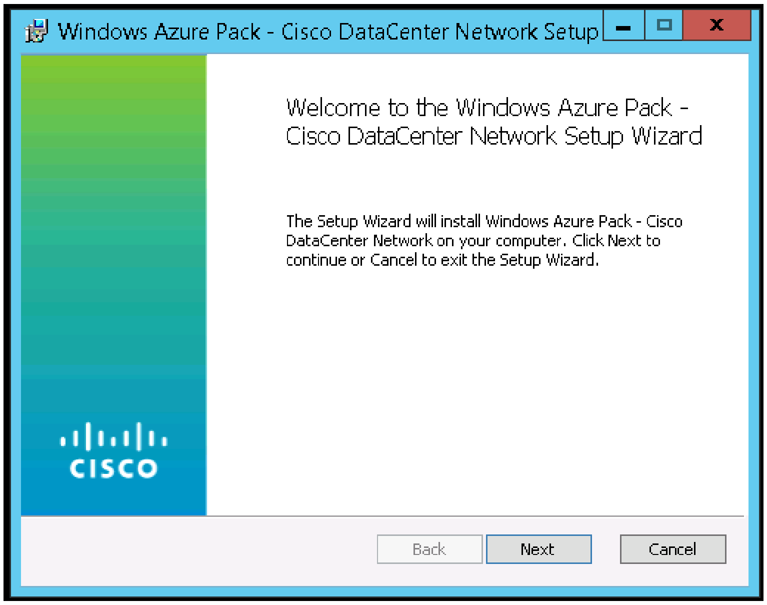
Caution Every time you install Cisco CNAP, the database is recreated. To preserve your data, you should always backup your database before reinstalling Cisco CNAP.

Note You can use the VBScript script packaged with Cisco CNAP to install it. The advantage of using a script is that you can specify various parameters, such as run in quiet mode, produce logs that can be useful in debugging installation issues, etc. For more information, see Appendix A—Using a Script to Install Cisco Cloud Network Automation Provisioner.

Step 1 Double-click the **CiscoCloudNetworkAutomationProvisioner.msi** Windows installer package. This can be run with any of the normal msi switches or can be launched with the msiexec command with any of the normal switches. Logging can be enabled with any of these options.

You see the Network Setup Wizard Welcome screen.

Figure 1-5 Network Setup Wizard Welcome Screen



Windows Azure Pack - Cisco DataCenter Network Setup

Welcome to the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

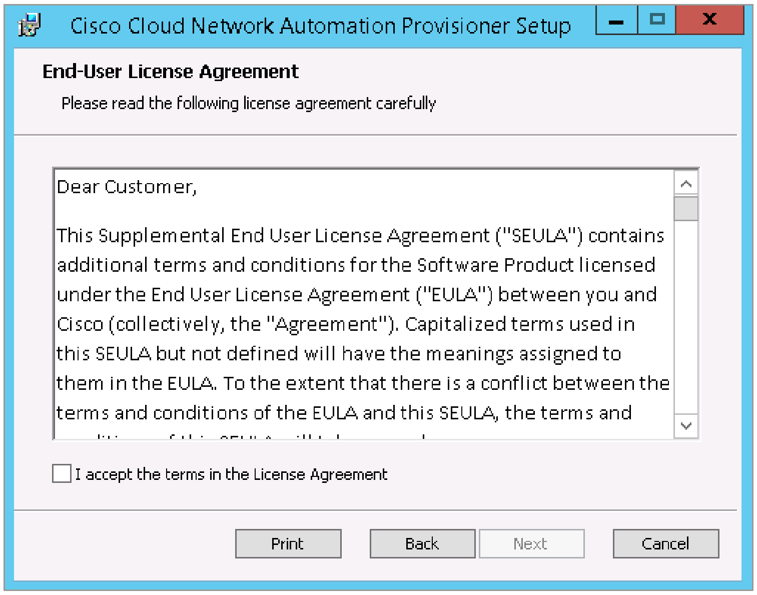
The Setup Wizard will install Windows Azure Pack - Cisco DataCenter Network on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Step 2 Click **Next**.

You see the End-User License Agreement screen, which has two sections you should read.

The first section is the Supplemental End User License Agreement (SEULA), the first part of which is shown in the screen below.

Figure 1-6 Supplemental End User License Agreement



End-User License Agreement

Please read the following license agreement carefully

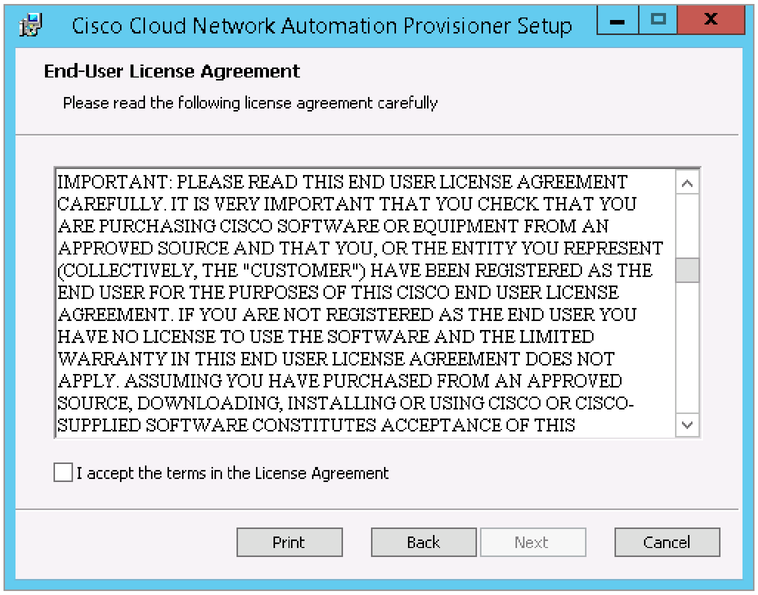
Dear Customer,

This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between you and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and

□ I accept the terms in the License Agreement

Scroll down to see the second section, the End User License Agreement (EULA), the first part of which is shown in the screen below.

Figure 1-7 End User License Agreement



End-User License Agreement

Please read the following license agreement carefully

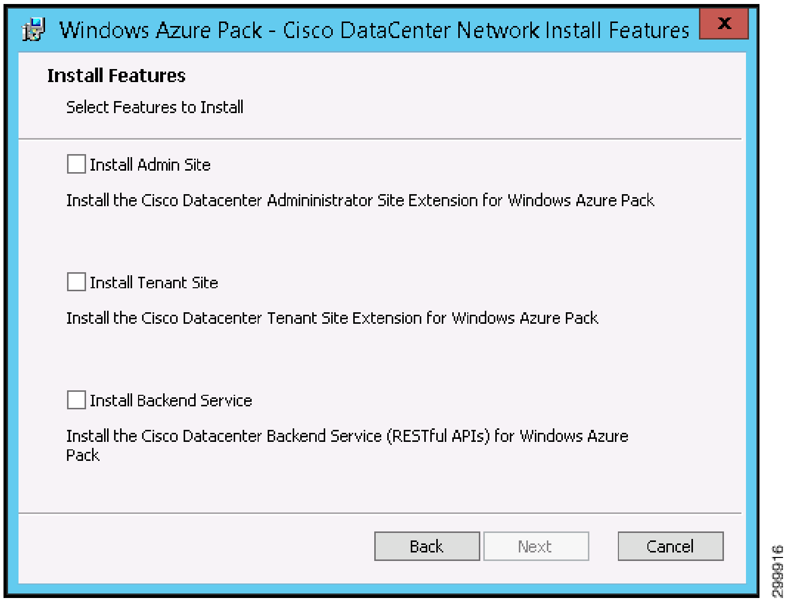
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS

□ I accept the terms in the License Agreement

Step 3 Click the box to accept the terms of the license agreement and click **Next**.

You see the Install Features screen.

Figure 1-8 Install Features Screen



Windows Azure Pack - Cisco DataCenter Network Install Features

Install Features

Select Features to Install

□ Install Admin Site

Install the Cisco Datacenter Admininistrator Site Extension for Windows Azure Pack

□ Install Tenant Site

Install the Cisco Datacenter Tenant Site Extension for Windows Azure Pack

□ Install Backend Service

Install the Cisco Datacenter Backend Service (RESTful APIs) for Windows Azure Pack

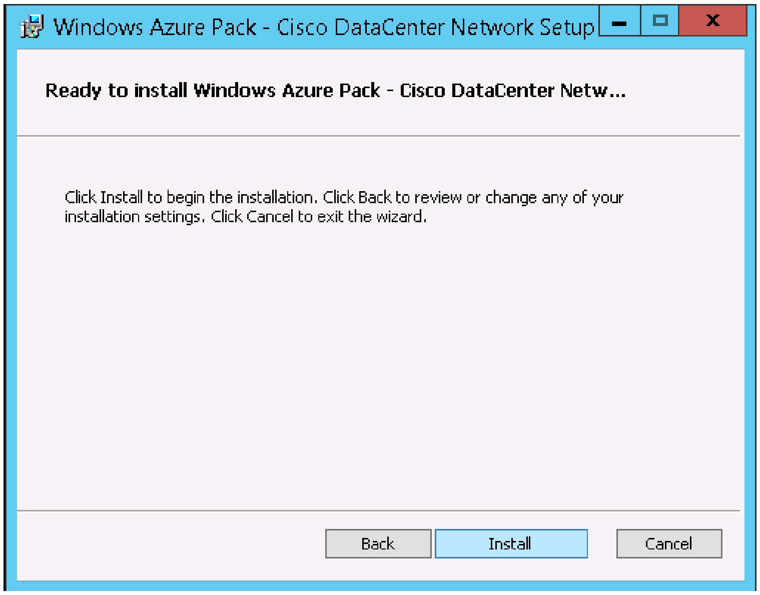
Note If you initially install only one or two features rather than all three, you cannot rerun the installer to install the remaining feature(s) you did not initially install. You must first remove the initial installation. For more information, see Removing an Installation.

Note If you did a WAP express install so that all three of these features will run on the same server, then you **must** install all three features at the same time. If the Tenant Site will run on one server and the Admin Site and Backend Service will be installed on a separate server, then install the Tenant Site first on its server, then simultaneously install both the Admin Site and the Backend Service on their own server.

Installing the Tenant Site

Step 1 If you select Install Tenant Site and click **Next**, you see the Ready to Install screen.

Figure 1-9 Ready to Install Screen



Windows Azure Pack - Cisco DataCenter Network Setup

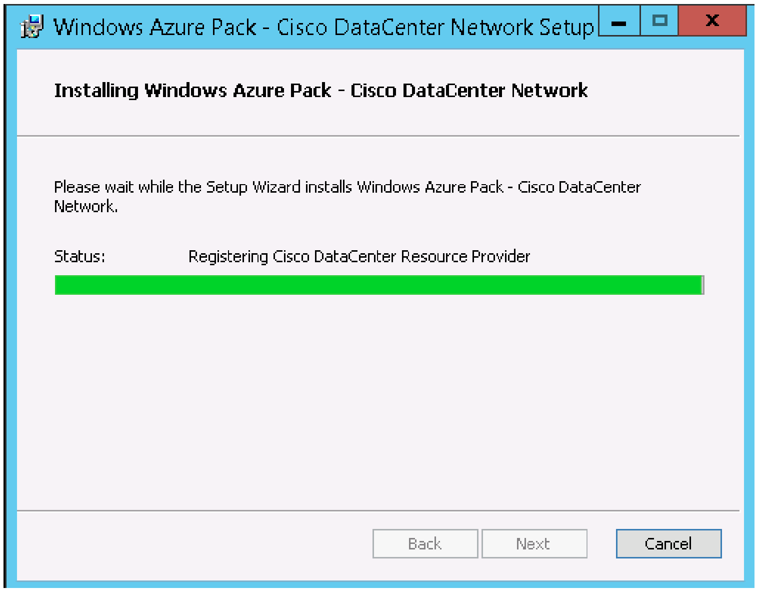
Ready to install Windows Azure Pack - Cisco DataCenter Netw...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 2 Click **Install**.

You see a screen with a status bar and messages indicating the progress of the installation.

Figure 1-10 Installation Progress Screen



Windows Azure Pack - Cisco DataCenter Network Setup

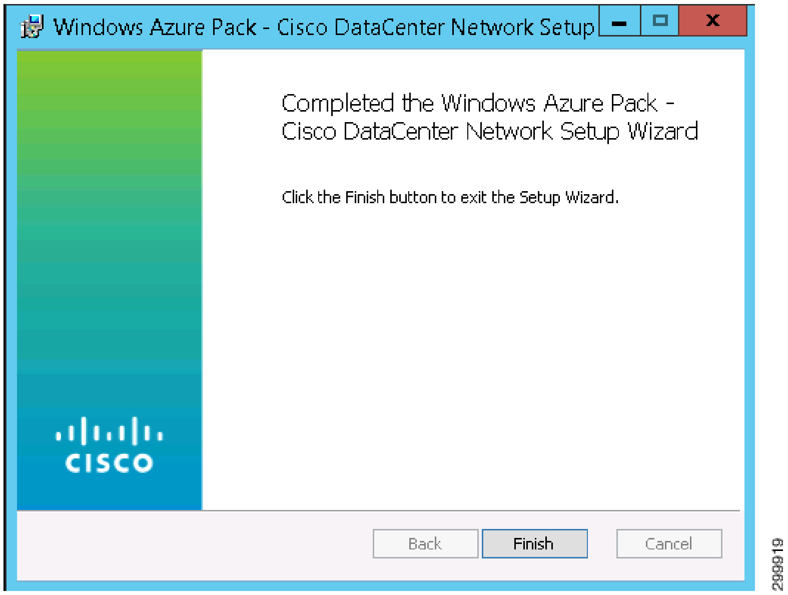
Installing Windows Azure Pack - Cisco DataCenter Network

Please wait while the Setup Wizard installs Windows Azure Pack - Cisco DataCenter Network.

Status: Registering Cisco DataCenter Resource Provider

When installation finishes, you see the Installation Complete screen.

Figure 1-11 Installation Complete Screen



Windows Azure Pack - Cisco DataCenter Network Setup

Completed the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

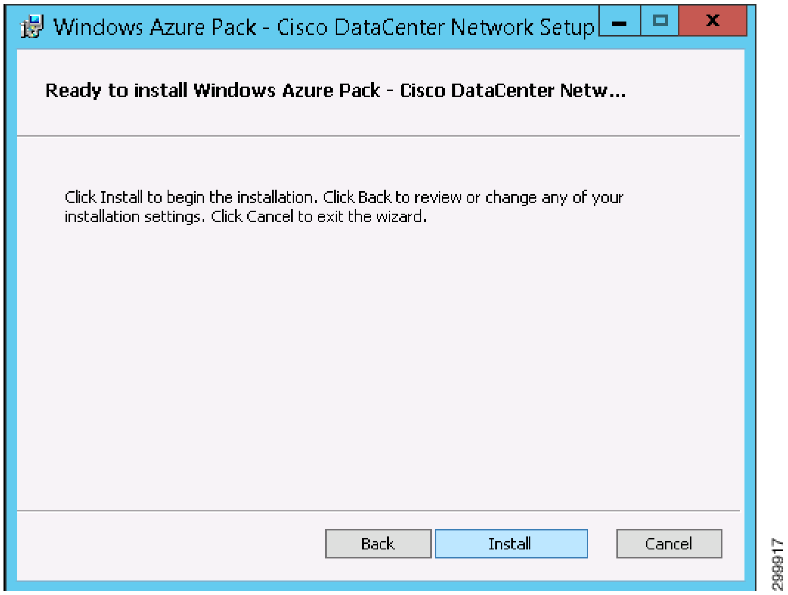
Click the Finish button to exit the Setup Wizard.

Step 3 Click **Finish** to exit.

Installing the Admin Site

Step 1 If you select Install Admin Site and click **Next**, you see the Ready to Install screen.

Figure 1-12 Ready to Install Screen



Windows Azure Pack - Cisco DataCenter Network Setup

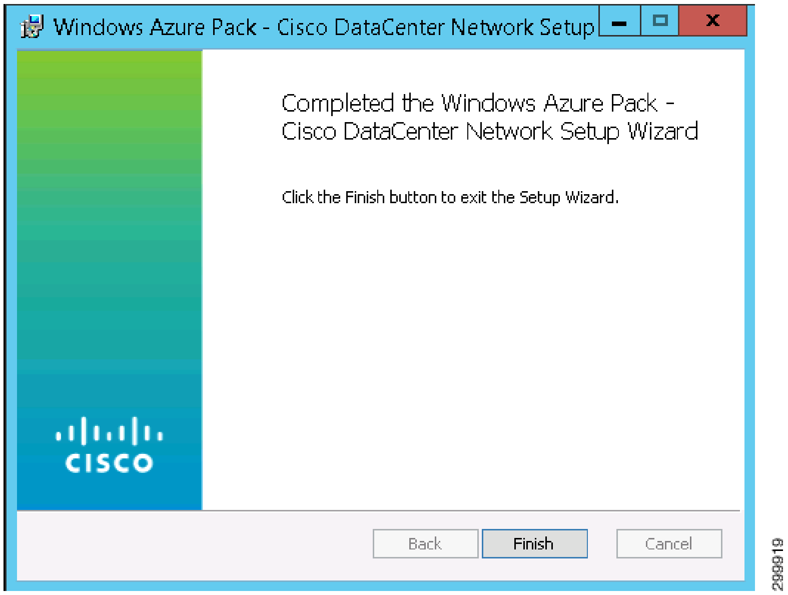
Ready to install Windows Azure Pack - Cisco DataCenter Netw...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 2 Click **Install**.

When installation finishes, you see the Installation Complete screen.

Figure 1-13 Installation Complete Screen



Completed the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

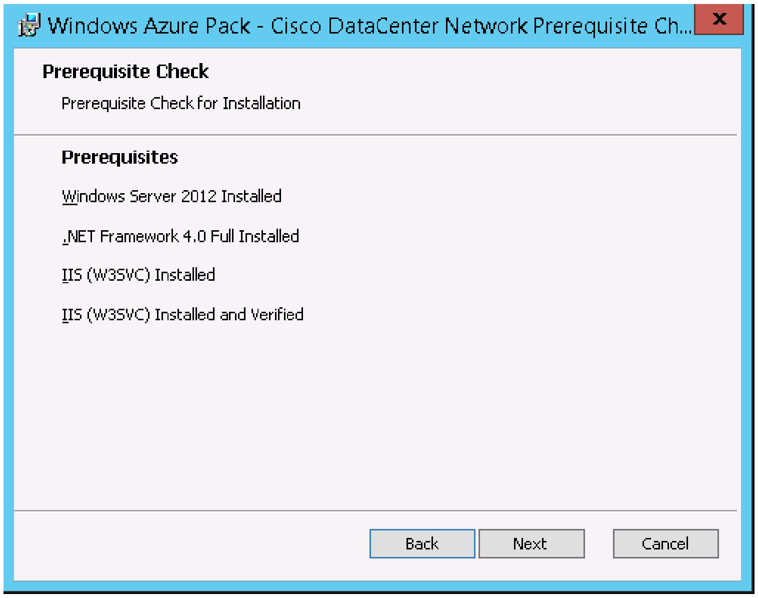
Click the Finish button to exit the Setup Wizard.

Step 3 Click **Finish** to exit.

Installing the Backend Service

Step 1 If you select Install Backend Service, when you click **Next** you see the Prerequisite Check screen.

Figure 1-14 Prerequisite Check Screen



Windows Azure Pack - Cisco DataCenter Network Prerequisite Ch...

Prerequisite Check

Prerequisite Check for Installation

Prerequisites

Windows Server 2012 Installed

.NET Framework 4.0 Full Installed

IIS (W3SVC) Installed

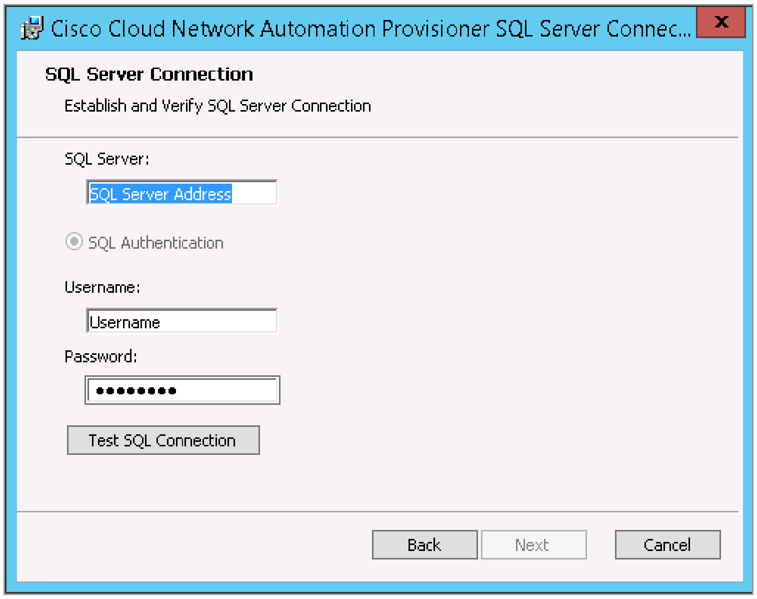
IIS (W3SVC) Installed and Verified

If one or more prerequisites are not met, you see error messages. Ensure all prerequisites are met before continuing.

Step 2 Click **Next**.

You see the SQL Server Connection screen.

Figure 1-15 SQL Server Connection Screen



Cisco Cloud Network Automation Provisioner SQL Server Connec...

SQL Server Connection

Establish and Verify SQL Server Connection

SQL Server: SQL Server Address

● SQL Authentication

Username: Username

Password: ●●●●●●●●●

Step 3 Complete the following fields:

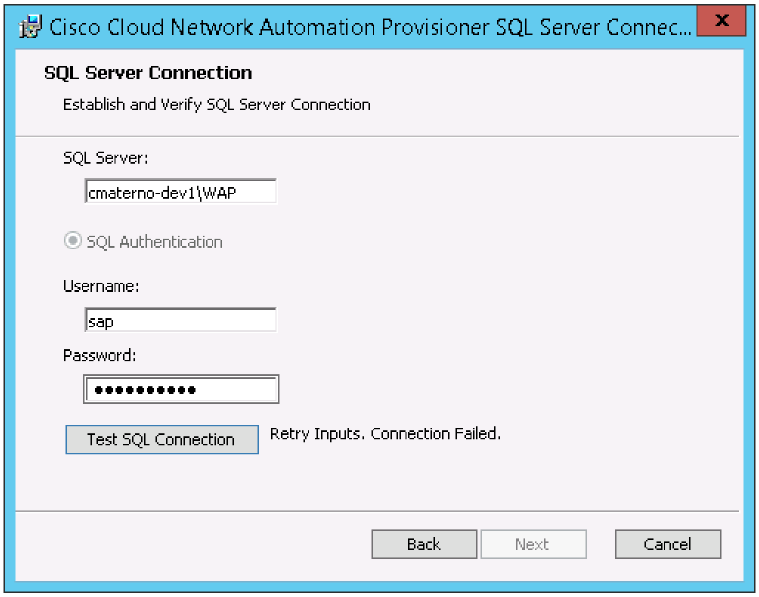
- **SQL Server:**—Enter the SQL connection string in the form *SQL server name\SQL instance*.
- **SQL Authentication** is the only option and is preselected.

- **Username:**—Enter your user ID for SQL authentication.
- **Password:**—Enter your password for SQL authentication.

Step 4 Click **Test SQL Connection**.

If the connection fails, you see the Retry Inputs. Connection Failed message.

Figure 1-16 SQL Server Connection Screen—Connection Failed Message



Cisco Cloud Network Automation Provisioner SQL Server Connec...

SQL Server Connection

Establish and Verify SQL Server Connection

SQL Server: cmaterno-dev1\WAP

● SQL Authentication

Username: sap

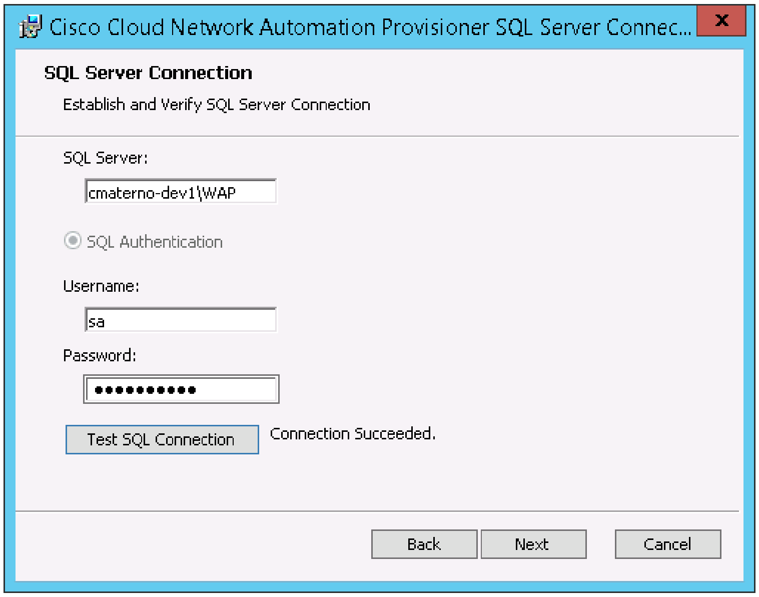
Password: ●●●●●●●●●●●

Retry Inputs. Connection Failed.

Step 5 Reenter the required information and click **Test SQL Connection**.

If you have entered the correct information, you see the Connection Succeeded message.

Figure 1-17 SQL Server Connection Screen—Connection Succeeded Message



Cisco Cloud Network Automation Provisioner SQL Server Connec...

SQL Server Connection

Establish and Verify SQL Server Connection

SQL Server: cmaterno-dev1\WAP

● SQL Authentication

Username: sa

Password: ●●●●●●●●●●●

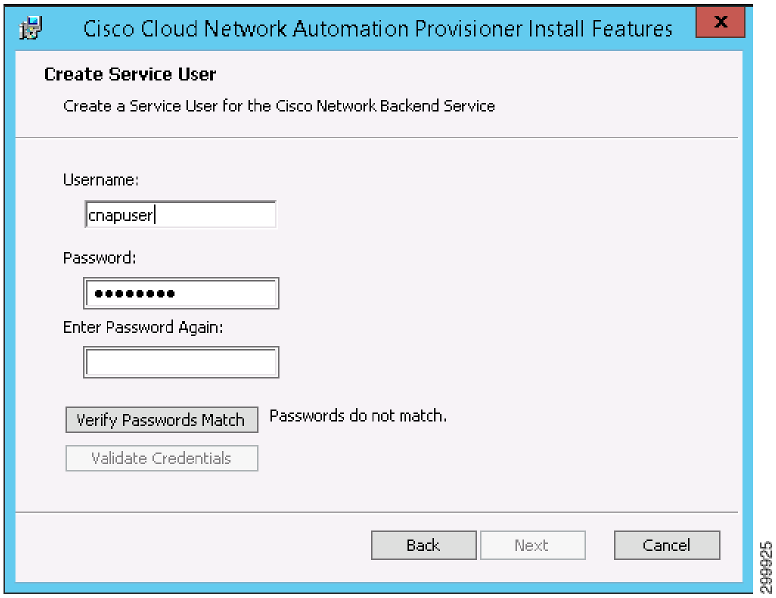
Connection Succeeded.

Step 6 When you see the Connection Succeeded message, click **Next**.

You see the Create Service User screen.

For security reasons, you must create a service user with credentials that are different than the Microsoft WAP credentials (in addition, the username **cannot** have a hyphen [-] in it).

Figure 1-18 Create Service User Screen



Create Service User

Create a Service User for the Cisco Network Backend Service

Username:

cnapuser

Password:

●●●●●●●●●

Enter Password Again:

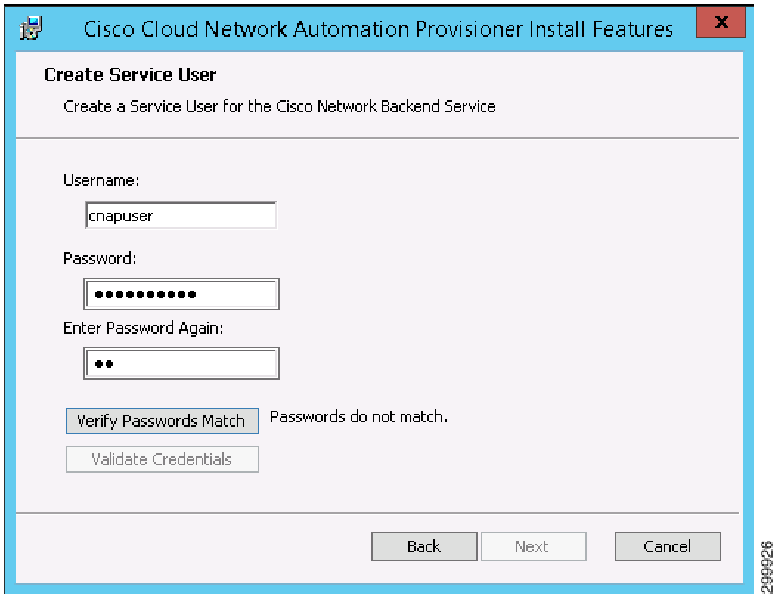
Passwords do not match.

Step 7 Complete the following fields (the installer automatically checks to ensure the user name is unique):

- **Username:**—Enter a username (the username **cannot** have a hyphen [-] in it).
- **Password:**—Enter a password.
- **Enter Password Again:**—Reenter the password.

Step 8 Click **Verify Passwords Match**. If they do not, you see the message Passwords do not match.

Figure 1-19 Create Service User Screen—Passwords Do Not Match Message



Cisco Cloud Network Automation Provisioner Install Features

Create Service User

Create a Service User for the Cisco Network Backend Service

Username: cnapuser

Password: ●●●●●●●●●●●

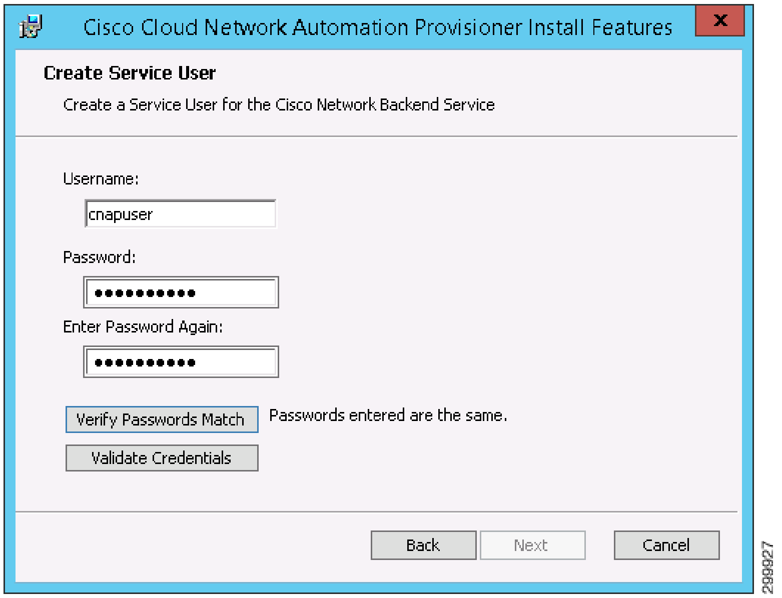
Enter Password Again: ●●

Passwords do not match.

Step 9 Reenter the password and click **Verify Passwords Match**.

If the passwords match, you see the message Passwords entered are the same.

Figure 1-20 Create Service User Screen—Passwords Match Message



Cisco Cloud Network Automation Provisioner Install Features

Create Service User

Create a Service User for the Cisco Network Backend Service

Username: cnapuser

Password: ●●●●●●●●●●●

Enter Password Again: ●●●●●●●●●●●

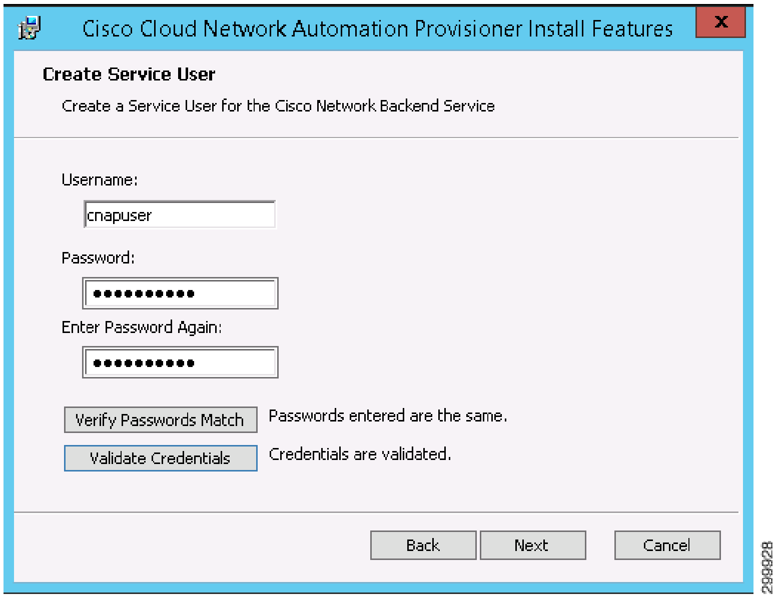
Passwords entered are the same.

Step 10 Click **Validate Credentials**. If the credentials are correct, you see the message Credentials are validated. If the credentials are not valid, the installer will time out and you will see a message indicating the issue:

- Password does not pass complexity check.
- User already exists at target.
- Credentials are invalid.
- Unable to verify.

If there is an error, correct the relevant item and again click **Validate Credentials**.

Figure 1-21 Create Service User Screen—Credentials are Validated Message



Cisco Cloud Network Automation Provisioner Install Features

Create Service User

Create a Service User for the Cisco Network Backend Service

Username: cnapuser

Password: ●●●●●●●●●●●

Enter Password Again: ●●●●●●●●●●●

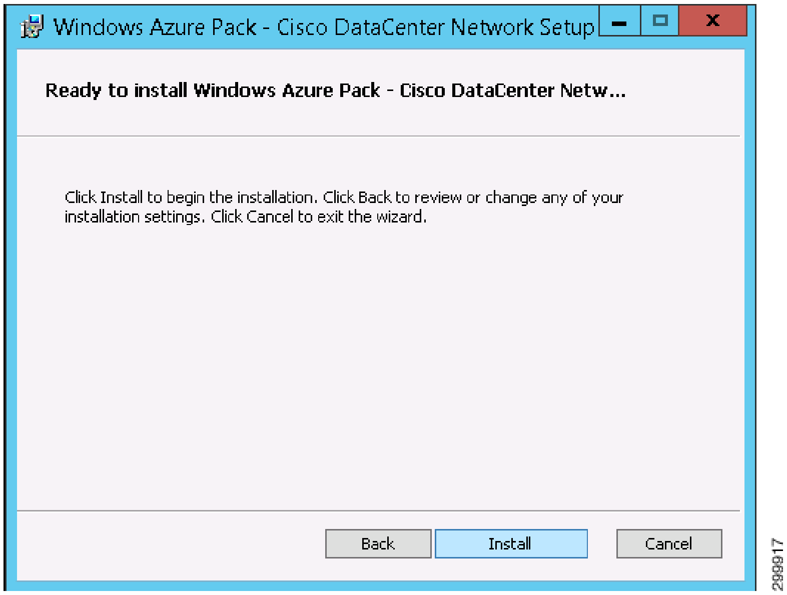
Passwords entered are the same.

Credentials are validated.

Step 11 Click **Next**.

You see the Ready to Install screen.

Figure 1-22 Ready to Install Screen



Windows Azure Pack - Cisco DataCenter Network Setup

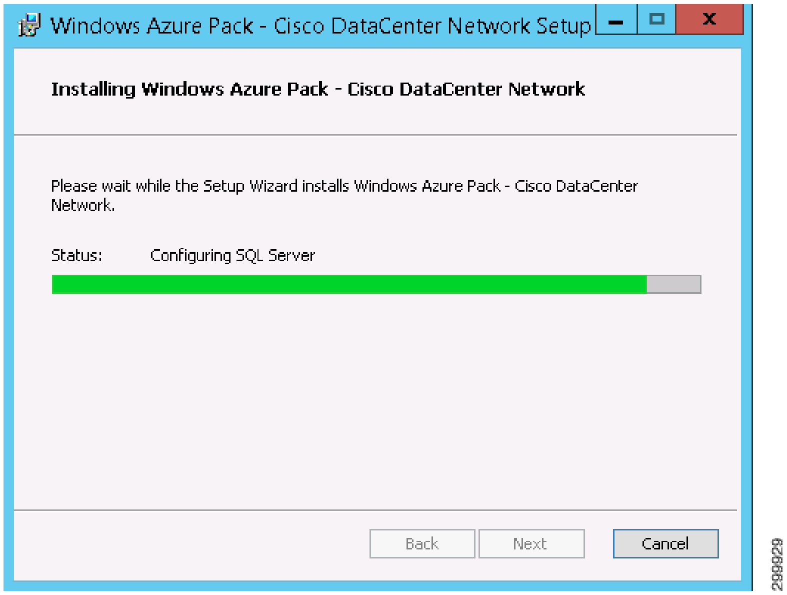
Ready to install Windows Azure Pack - Cisco DataCenter Netw...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 12 Click **Install**.

You see a screen with a status bar and messages indicating the progress of the installation.

Figure 1-23 Installation Progress Screen



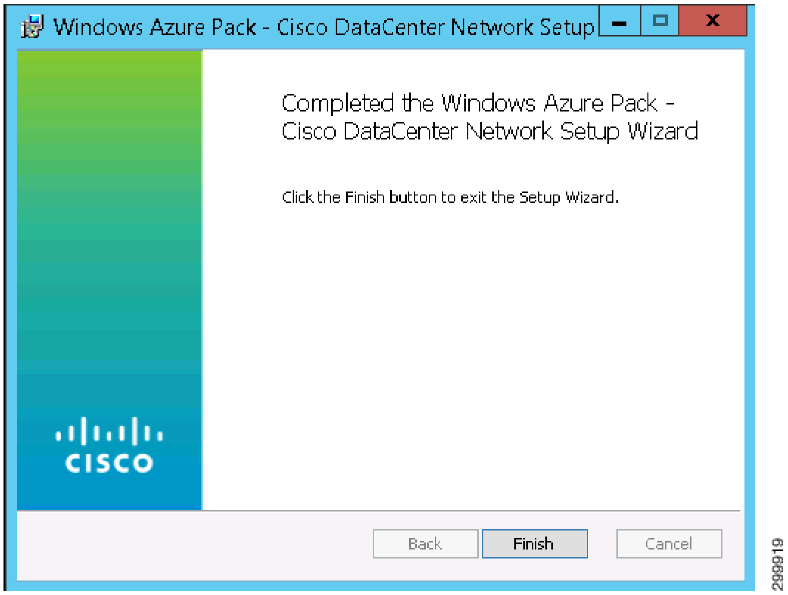
Installing Windows Azure Pack - Cisco DataCenter Network

Please wait while the Setup Wizard installs Windows Azure Pack - Cisco DataCenter Network.

Status: Configuring SQL Server

When installation finishes, you see the Installation Complete screen.

Figure 1-24 Installation Complete Screen



Completed the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 13 Click **Finish** to exit.

Post-installation Set Up Procedures

After installing Cisco CNAP, either using the installer GUI or the script described in Appendix A—Using a Script to Install Cisco Cloud Network Automation Provisioner you must complete the following post-installation procedures:

- Run the RegisterRP.ps1 file to register the resource provider.
- Log in to the Admin Portal and configure the global settings for the system.
- Start the Cisco.Network.Provisioner Windows Service.

Running the RegisterRP.ps1 File

You must run the RegisterRP.ps1 file via Windows PowerShell on the AdminAPI server to register the resource provider. The installer does not automatically do this.

Note The Cisco CNAP Admin site runs on port 30040 for HTTP and port 30041 for HTTPS communication.

Configuring Global Settings for the System

Note At this point, you are only required to enter the three Microsoft Service Provider Foundation (SPF) Connection settings, which let you connect to the SPF server to retrieve clouds. However we recommend that you set all global system parameters at this time.

Before you begin configuring global settings, complete the steps in the following sections as you will need this information to complete some fields

- Creating the Cisco CSR 1000V Template Used by Cisco CNAP
- Creating the Citrix NetScaler VPX Template Used by Cisco CNAP

Creating the Cisco CSR 1000V Template Used by Cisco CNAP

To create the Cisco CSR 1000V template:

Step 1 Obtain a supported Cisco CSR 1000V.

Step 2 Copy the ISO image into the library ISO location of the targeted VMM and refresh the library.

Step 3 Create a virtual machine with a blank virtual hard disk using the following configuration parameters (if not specified, the default configuration will be used):

- General hardware configuration:
  - One (1) CPU

    Note You can configure two (2) or four (4) CPUs. Cisco CNAP supports only one template and all Cisco CSR 1000Vs will be instantiated from the one template. See: http://www.cisco.com/c/en/us/products/collateral/routers/cloud-services-router-1000v-series/datasheet-c78-733443.html.

  - 4 GB memory
- Hardware bus configuration:
  - Virtual hard disk type is fixed and size is 8GB
  - Virtual DVD driver connecting to the Cisco CSR 1000V ISO you provided
- Hardware network adapters configuration:
  - Add seven (7) additional network adapters and change all eight (8) adapters' MAC addresses to static.
- Advanced hardware configuration:
  - Enable high availability and set priority to **High**.
  - Change CPU priority to **High**.
  - Change Memory weight to **High**.

Step 4 Boot the virtual machine and follow the prompt to create a default (blank) configuration for the Cisco CSR 1000V.

Step 5 Shut down the virtual machine and disconnect the ISO image from the virtual machine virtual DVD driver.

Step 6 In VMM, convert the virtual machine into a virtual machine template.

Creating the Citrix NetScaler VPX Template Used by Cisco CNAP

To create the Citrix NetScaler VPX template:

Step 1 Download the Citrix NetScaler Virtual Appliance setup files:

a. In a web browser, go to http://www.citrix.com and click **My Citrix**.

b. Type your username and password.

c. Click **Downloads**.

d. In search downloads by Product, select **NetScaler**.

e. Under Virtual Appliances, click **Netscaler VPX**.

f. Copy the compressed file to your server.

Step 2 Create the template:

a. Extract the contents of the compressed file.

b. There is a folder for Virtual Hard Disks that contains the VHD file, which by default is named “dynamic”. You can rename it.

c. Copy the VHD to the VMM library.

d. Refresh the VMM library and ensure you see the new VHD.

e. Right-click the VHD and select **Create VM Template**.

f. Set the number of processor to two (2).

g. Set the RAM to 2048.

h. Be default there is only one network adapter. Add one more. The first network adapter is used for management connectivity and the second one is used for the data path.

i. Change all adapters' (two total) MAC addresses to static.

j. Set the VM to Highly Available.

k. Finish the creation process.

In summary, you create a virtual machine template with the VHD file using the following configuration parameters (if not specified, the default configuration will be used):

- General hardware configuration:
  - Two (2) CPUs
  - 2 GB memory
- Hardware network adapters configuration:
  - Add one (1) additional network adapter and change all two (2) adapters' MAC addresses to static.
- Advanced hardware configuration:
  - Enable high availability and set priority to **High**.
  - Change CPU priority to **High**.
  - Change Memory weight to **High**.

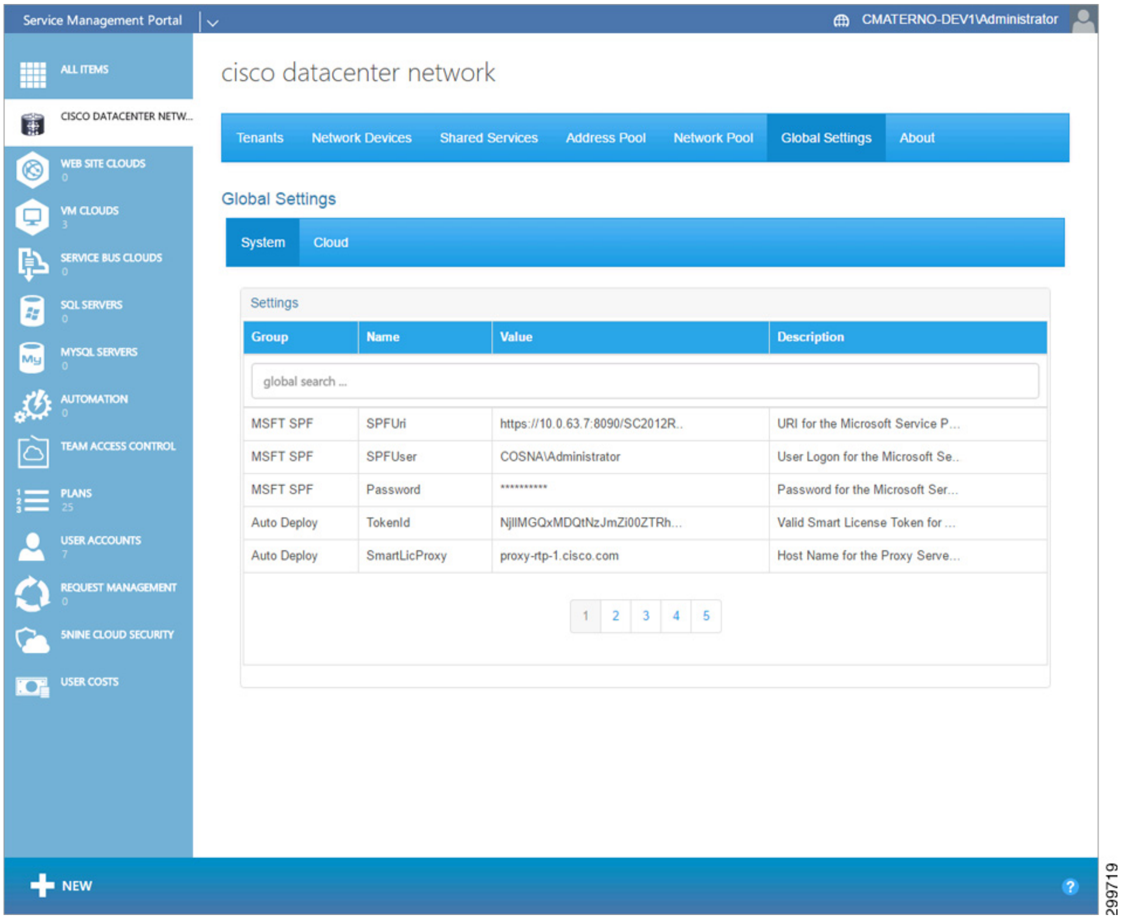
Configuring Global System Settings

Note You only need to perform this step once.

Step 1 On the Tenants tab, click the **Global Settings** tab.

You see the Global System Settings screen, as shown in the following screen.

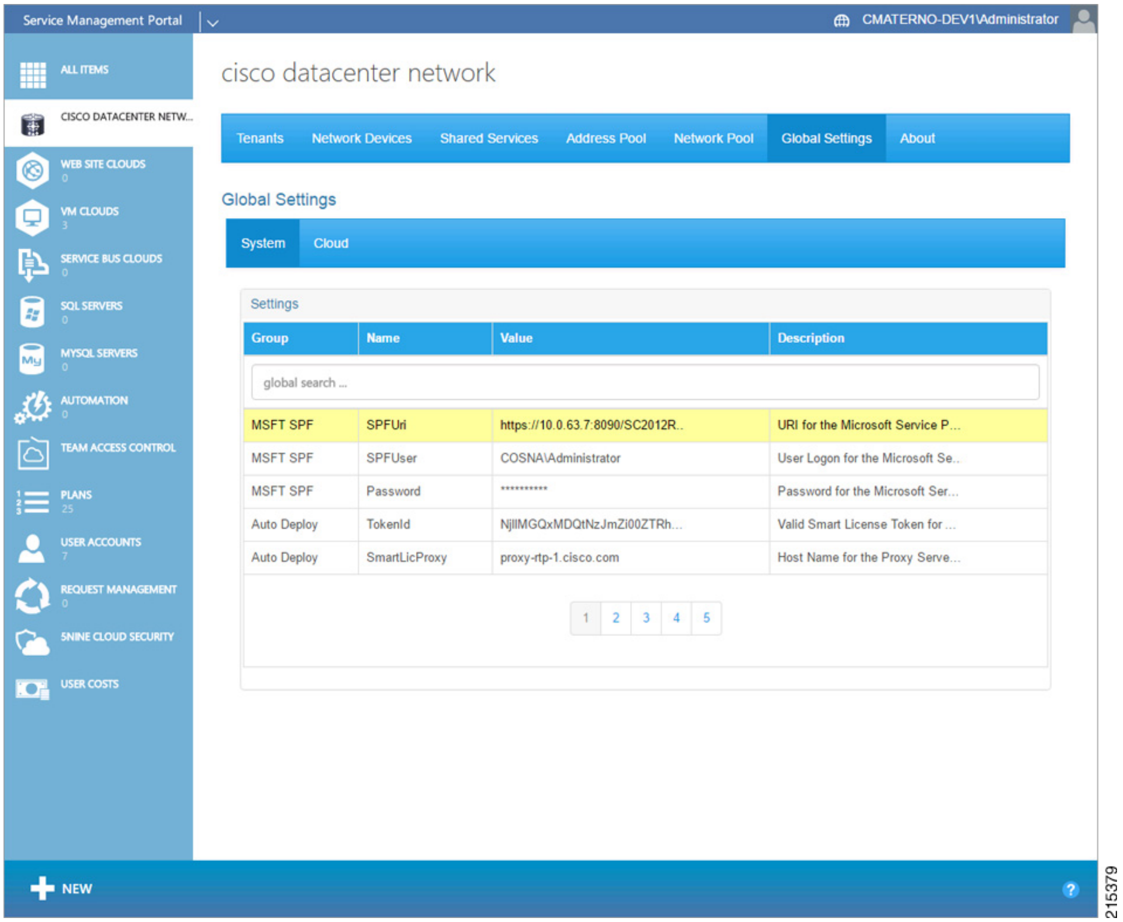
Figure 1-25 Global System Settings Screen



Group	Name	Value	Description
MSFT SPF	SPFUri	https://10.0.63.7:8090/SC2012R..	URI for the Microsoft Service P...
MSFT SPF	SPFUser	COSNA\Administrator	User Logon for the Microsoft Se..
MSFT SPF	Password	**********	Password for the Microsoft Ser...
Auto Deploy	TokenId	NjllMGQxMDQtNzJmZi00ZTRh...	Valid Smart License Token for ...
Auto Deploy	SmartLicProxy	proxy-rtp-1.cisco.com	Host Name for the Proxy Serve...

Step 2 Move the cursor over the first row of the settings table and the row is highlighted, as shown in the following screen.

Figure 1-26 Global System Settings Screen—Row Highlighted

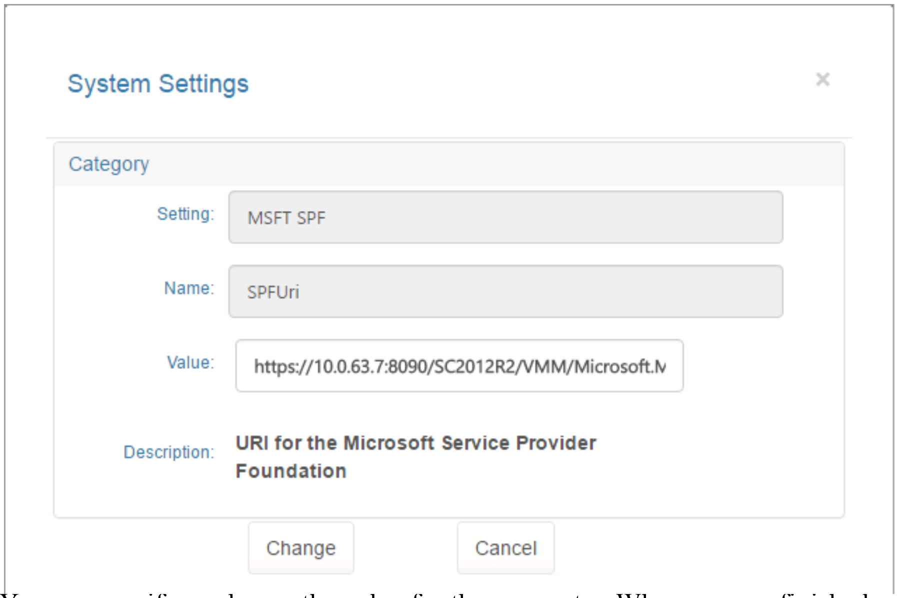


Group	Name	Value	Description
MSFT SPF	SPFUri	https://10.0.63.7:8090/SC2012R..	URI for the Microsoft Service P...
MSFT SPF	SPFUser	COSNA\Administrator	User Logon for the Microsoft Se..
MSFT SPF	Password	**********	Password for the Microsoft Ser...
Auto Deploy	TokenId	NjllMGQxMDQtNzJmZi00ZTRh...	Valid Smart License Token for ...
Auto Deploy	SmartLicProxy	proxy-rtp-1.cisco.com	Host Name for the Proxy Serve...

Step 3 Click the highlighted row.

You see a pop-up window, as shown in the following screen.

Figure 1-27 Global System Settings Screen—Parameter Pop-up Window



System Settings

Category

Setting: MSFT SPF

Name: SPFUri

Value: https://10.0.63.7:8090/SC2012R2/VMM/Microsoft.M

Description: URI for the Microsoft Service Provider Foundation

Step 4 You can specify or change the value for the parameter. When you are finished, click **Change**. Click **Cancel** to return to the previous screen without entering/changing any values.

Step 5 Highlight each row in turn and specify or change the value for each parameter in the pop-up windows. When you are finished with the parameters on the first screen, click **2** at the bottom of the screen to see the next set of values.

There are four screens where you can specify/change System Global Settings. Table 1-2 describes the various fields and their possible values.

Table 1-2 Global System Settings

Group	Name	Sample Values[1]	Description
MSFT SPF	SPFUri	https://{*spf-server-name*}:8090/SC2012/{provider-service}/{subscription-id}/Microsoft.Management.Odata.svc/	URI for the Microsoft Service Provider Foundation
MSFT SPF	SPFUser	*<domain>\<user name>*	User logon for the Microsoft Service Provider Foundation
MSFT SPF	Password	*********	Password for the Microsoft Service Provider Foundation
Auto Deploy	TokenID	<Token-string>	Valid Smart License Token for Cisco CRS1000V auto deployment
Auto Deploy	SmartLicProxy		Host Name for the Proxy Server Used for Smart Licensing Validation
Auto Deploy	SmartLicProxyPort		TCP Port for the Proxy Server Used for Smart Licensing Validation
Auto Deploy	PSHost	*n.n.n.n*	FQN/IP Address of System Center VMM Host
Auto Deploy	PSUser	*<domain>\<user name>*	User Logon for the Microsoft System Center VMM
Auto Deploy	PSPassword		Password for the Microsoft System Center VMM
Auto Deploy	CSRVmTemplateName	csr1000vfixeddisk	Name of the Cisco CSR 1000V VM Template. For more information, see Creating the Cisco CSR 1000V Template Used by Cisco CNAP.
Auto Deploy	NSVmTemplateName	netscaler1000vfixeddisk	Name of the Citrix NetScaler VPX VM Template. For more information, see Creating the Citrix NetScaler VPX Template Used by Cisco CNAP.
Auto Deploy	ISODestinationFolder	vmm Library on VMM management Server For example: VMMServ-er01\SEALibrary	Folder at the System Center VMM Host to hold Post deployment ISOs
Auto Deploy	CSRUser	admin	Administrator User Logon set at BOOTSTRAP of the Cisco CSR 1000V
Auto Deploy	CSRPassword	********	Administrator Password set at BOOTSTRAP of the Cisco CSR 1000V. You can change the password when initially defining global settings. Follow good security practices to set a secure password. However once you have onboarded devices, you **cannot** change the password since that will cause container creation to fail.
Auto Deploy	NSUser	nsroot	Administrator User Logon at BOOTSTRAP of the Citrix NetScaler VPX
Auto Deploy	NSRPassword	******	Administrator Password set at BOOTSTRAP of the Citrix NetScaler VPX

Table 1-2 Global System Settings

Auto Deploy	VMMgmtNetworkName	MgmtVL0046VMNetwork	VMNetwork used for management of the Cisco CSRs and Citrix NetScaler VPXs. This is not the Logical Switch.
Auto Deploy	NameServer	10.0.43.10	Name Server Address for Virtual Network Devices
Auto Deploy	MgmtDomain	vmdc-cosn.cisco.com	Domain name defined on the Management Network
Auto Deploy	VMConfigFileFolder	C:\CNAPTemp\	This directory must be created before creating containers; if this directory is not present, container creation will fail. Directory on the Admin Portal server where the Cisco CSR 1000V and Citrix NetScaler VPX ISOs are created before they are copied to the Microsoft SCVMM. The default is “c:\temp\”. If you change the default, ensure that you include a trailing “\” on the end of the path name.
Auto Deploy	SyslogServer	10.0.63.231	Syslog Server address for Virtual Network Devices

[1] The values shown are examples. Use values appropriate for your cloud environment.

Starting the Cisco.Network.Provisioner Windows Service

The Cisco.Network.Provisioner Windows Service is installed as part of the Cisco CNAP installation process, however it is not started automatically since the SPF connection settings must first be set.

Locate and start the Cisco.Network.Provisioner Windows Service.

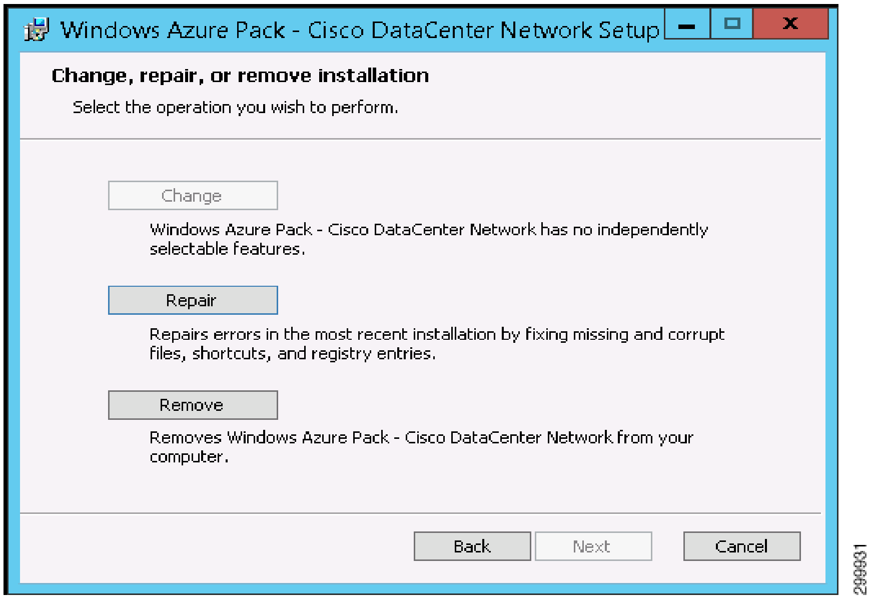
Removing an Installation

If you initially install one or two features, you cannot rerun the installer to install the remaining features you did not initially install. You must first remove the initial installation.

Not enabled in the current release: If you find anomalies in your installation, you should first try to repair the installation to see if the anomalies are resolved. If the repair does not resolve the problems, first remove the installation and then reinstall it.

After an installation, if you double-click the **CiscoCloudNetworkAutomationProvisioner.msi** Windows installer package, you see the Change, Repair, or Remove Installation screen.

Figure 1-28 Change, Repair, or Remove Installation Screen



Windows Azure Pack - Cisco DataCenter Network Setup

Change, repair, or remove installation

Select the operation you wish to perform.

Change

Windows Azure Pack - Cisco DataCenter Network has no independently selectable features.

Repair

Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.

Remove

Removes Windows Azure Pack - Cisco DataCenter Network from your computer.

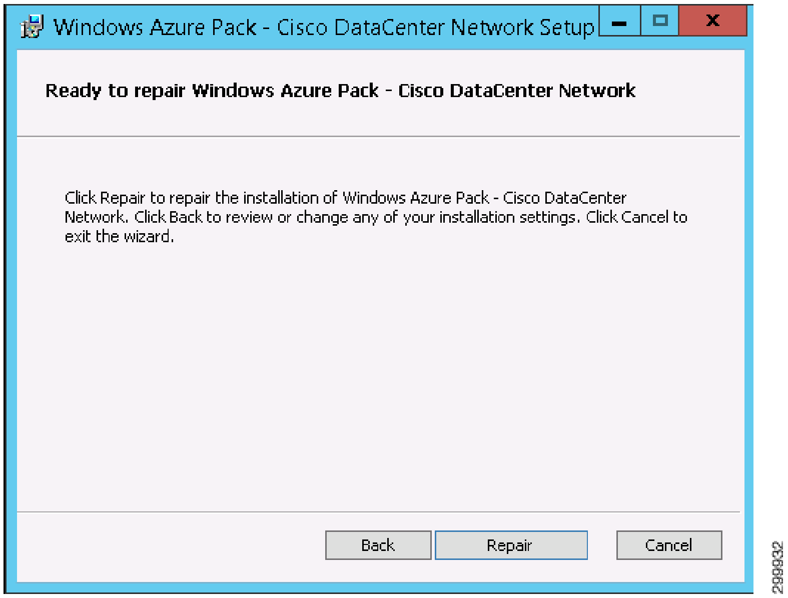
Note The Change button is not active for the reason indicated on the screen.

Repairing an Installation

Note Not enabled in the current release.

Step 1 To repair an installation, click **Repair**. You see the Ready to Repair an Installation screen.

Figure 1-29 Ready to Repair an Installation Screen



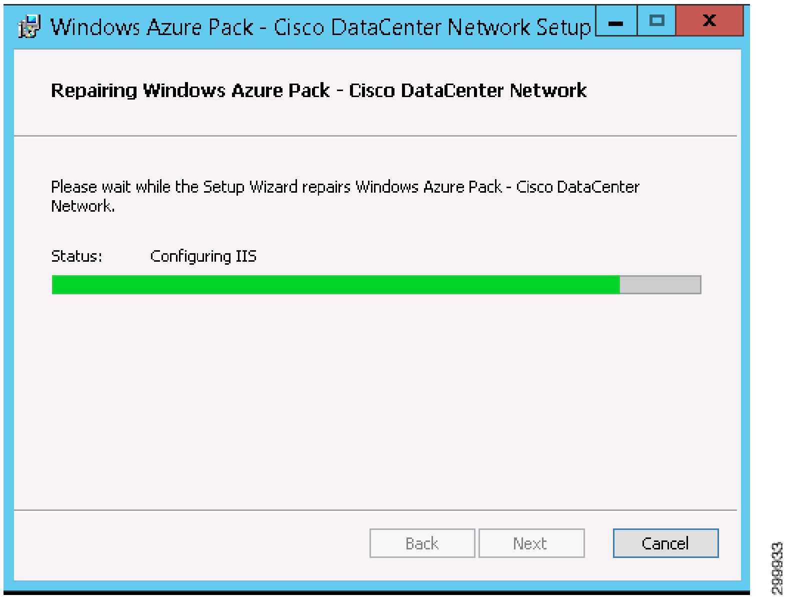
Ready to repair Windows Azure Pack - Cisco DataCenter Network

Click Repair to repair the installation of Windows Azure Pack - Cisco DataCenter Network. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 2 Click **Repair**.

You see a screen with a status bar and messages indicating the progress of the installation repair.

Figure 1-30 Progress of Installation Repair Screen



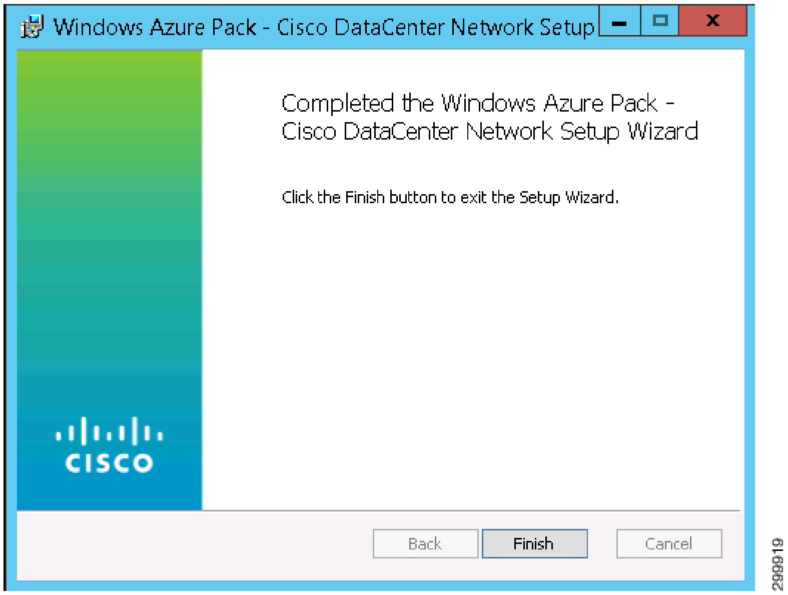
Repairing Windows Azure Pack - Cisco DataCenter Network

Please wait while the Setup Wizard repairs Windows Azure Pack - Cisco DataCenter Network.

Status: Configuring IIS

When the repair completes, you see the Repair Complete screen.

Figure 1-31 Repair Complete Screen



Completed the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

Click the Finish button to exit the Setup Wizard.

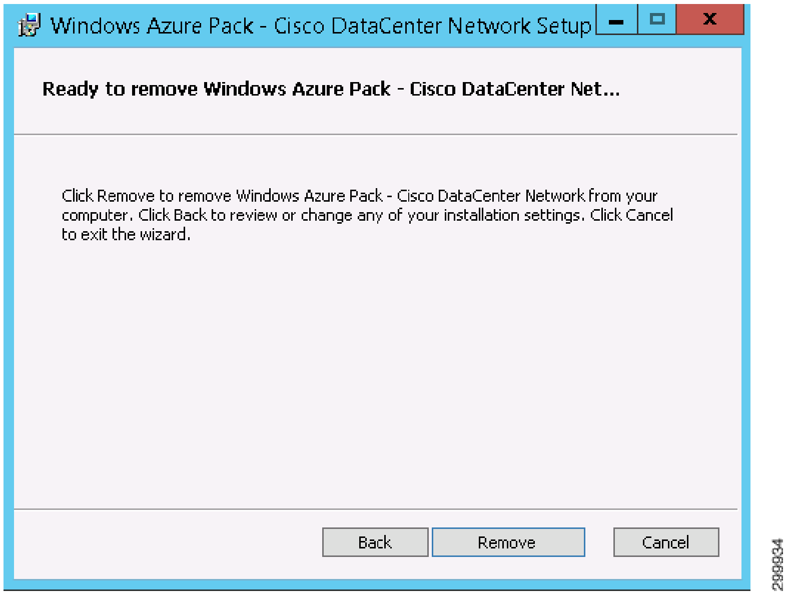
Step 3 Click **Finish** to exit.

Removing an Installation

Note Put a note about WAP Express v/s DIstributed WAP install. In a WAP Express installation, all components are installed on the same machine so you only need to run remove once. In a WAP Distributed installation, you must remove the components from all individual servers

Step 1 To remove an installation, click **Remove**. You see the Ready to Remove an Installation screen.

Figure 1-32 Ready to Remove an Installation Screen



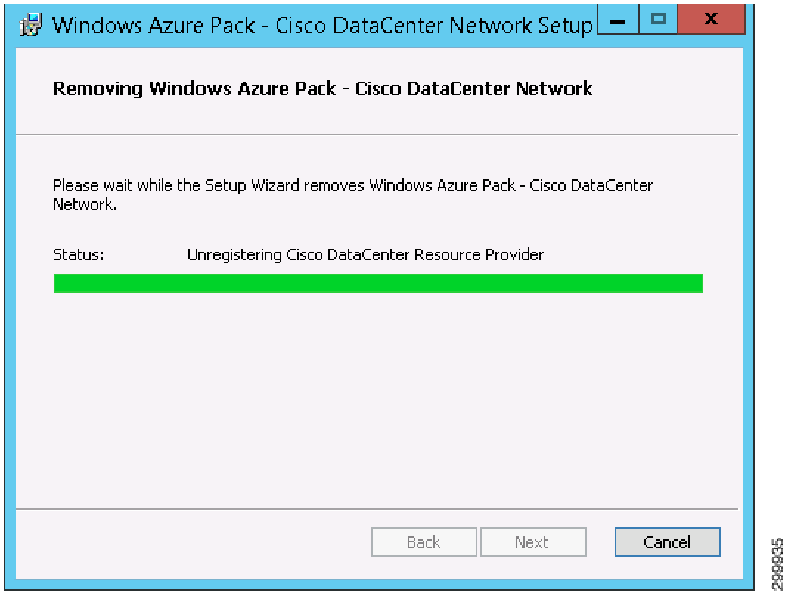
Ready to remove Windows Azure Pack - Cisco DataCenter Net...

Click Remove to remove Windows Azure Pack - Cisco DataCenter Network from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Step 2 Click **Remove**.

You see a screen with a status bar and messages indicating the progress of the installation removal.

Figure 1-33 Progress of Installation Removal Screen



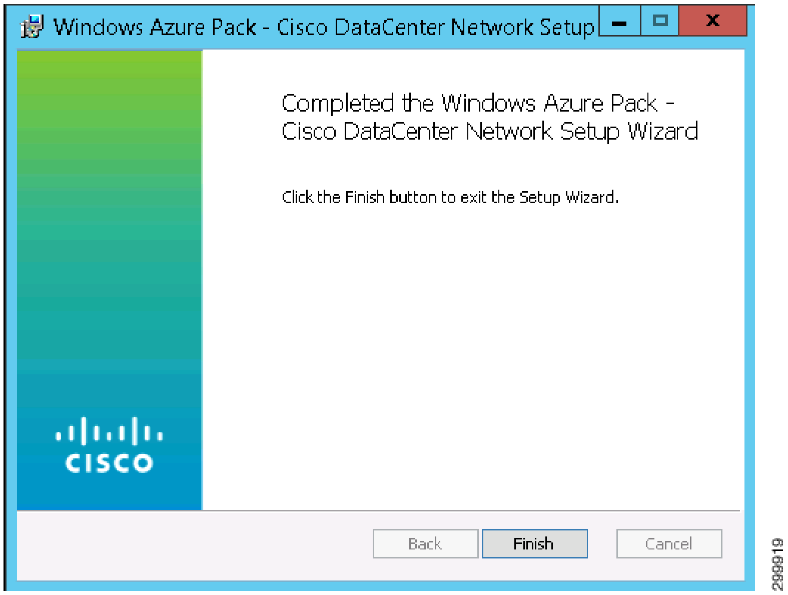
Removing Windows Azure Pack - Cisco DataCenter Network

Please wait while the Setup Wizard removes Windows Azure Pack - Cisco DataCenter Network.

Status: Unregistering Cisco DataCenter Resource Provider

When the removal completes, you see the Remove Complete screen.

Figure 1-34 Remove Complete Screen



Windows Azure Pack - Cisco DataCenter Network Setup

Completed the Windows Azure Pack - Cisco DataCenter Network Setup Wizard

Click the Finish button to exit the Setup Wizard.

Step 3 Click **Finish** to exit.

Installing Cisco Network Services Orchestrator Enabled by Tail-f

Note You must install version 4.1.1.

This is a summary of the Cisco NSO installation process. For more detailed information, when the Cisco NSO tar file is expanded, there is a documentation folder containing various documents that you should consult (/opt/ncs/current/doc/pdf).

Note Refer to the Cisco NSO High Availability (HA) deployment guide to set up Cisco NSO in HA mode. The HA guide is part of the tailf-hcc High Availability Framework package.

Note When onboarding a Cisco APIC on the Network Devices tab in the Admin Portal, the Cisco APIC expects the same Linux username and password credentials as those of the Cisco NSO. You must ensure such a Linux user exists on the Cisco NSO.

Note *Before* you onboard a Cisco APIC on the Network Devices tab in the Admin Portal, you **must** create a directory to store the Cisco APIC configurations. As the admin user (or ensure the admin user has read and write access to the directory), create the directory:
/home/admin/cisco-apicdc

Installing Required Network Element Drivers

Note You should always consult the *Release Notes for Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1* to obtain the most up-to-date list of required network element drivers (NEDs).

Consult the Cisco NSO documentation for instructions on installing NEDs.

Install these NEDs:

Name	Package Version
cisco-apicdc	3.0.2
cisco-asa	4.0.1
cisco-ios	4.0.2
cisco-iosxr	4.0.1
citrix-netscaler	3.0.5
tailf-hcc	4.0.1

Note Whenever you update the NEDs, you should issue the following command to restart Cisco NSO service:
# **/etc/init.d/ncs restart-with-package-reload**

Connecting Cisco Cloud Network Automation Provisioner to the Cisco Network Services Orchestrator

Allowing Manual Configuration Changes on Devices Managed by Cisco CNAP

All devices managed by Cisco CNAP are registered with Cisco NSO, including the Cisco APIC, WAN PEs, and Cisco ASA firewalls. Cisco CNAP maintains a copy of device configurations in a Configuration Database (CDB), which is a component of Cisco NSO. By default Cisco NSO monitors the configurations of devices and expects them to be synchronized with the configurations in its CDB. Configuration synchronization is checked before configuration changes and if an out-of-synchronization condition is detected, an error condition will occur. When Cisco NSO is run in this default mode, all configuration changes on devices in Cisco NSO have to be pushed via the Cisco NSO interface. Manually configuring any device directly through its native interface, such as CLI, will cause Cisco NSO to error out and stop all automated provisioning via Cisco CNAP.

Since some configuration may need to be done on data center network infrastructure devices outside of Cisco CNAP and SP administrators may prefer to directly configure devices using native interfaces, such as CLI, instead of the Cisco NSO interface, a command must be issued to not require the Cisco NSO CDB to be kept in synchronization with the entire configuration of the device. To be able to configure a device from both Cisco CNAP (via Cisco NSO) and directly from its native interface, the **out-of-sync-commit-behavior** parameter must be set to **accept** in Cisco NSO, which lets Cisco NSO push configurations to devices even if they are out of synchronization.

Note To avoid Cisco CNAP errors and malfunctions, direct manual configuration changes to devices must be carefully performed to avoid interference with Cisco CNAP-pushed configurations.

The **out-of-sync-commit-behavior** parameter is a Cisco NSO global setting which applies to all devices added in Cisco NSO. Manually issue the following command on the Cisco NSO immediately *after* installing Cisco NSO and *before* adding Cisco NSO to Cisco CNAP.

```
set devices global-settings out-of-sync-commit-behaviour accept
```

Note Since Cisco CNAP is also pushing configurations for the automation of work flows on devices, certain precautions need to be followed when manually configuring devices to avoid disrupting Cisco CNAP-based automation. Changing configurations pushed from Cisco CNAP will cause the automated provisioning system to malfunction, which in some cases could cause all automated provisioning to stop until the error conditions are manually remediated. In general on the data center provider edge, all configurations under the tenant VRFs pushed by Cisco CNAP should not be edited or changed, including sub-interfaces and routing. Similarly on the Cisco APIC, the Cisco APIC tenants configured by Cisco CNAP should only be changed by Cisco CNAP. Any configurations pushed by Cisco CNAP should not be manually edited.

Connecting Cisco CNAP to Cisco NSO

Note To support Cisco CSR 1000V IOS XE Software Versions 03.16 and 03.17, you have to add another global setting on the Cisco NSO:
set devices global-settings read-timeout 60

Note All global settings done on the Cisco NSO in HA mode need to be executed on all master and slave nodes in the HA cluster.

To connect Cisco CNAP to Cisco NSO, you must add the Cisco NSO in the Admin Portal. The Cisco NSO should be the first network device you add.

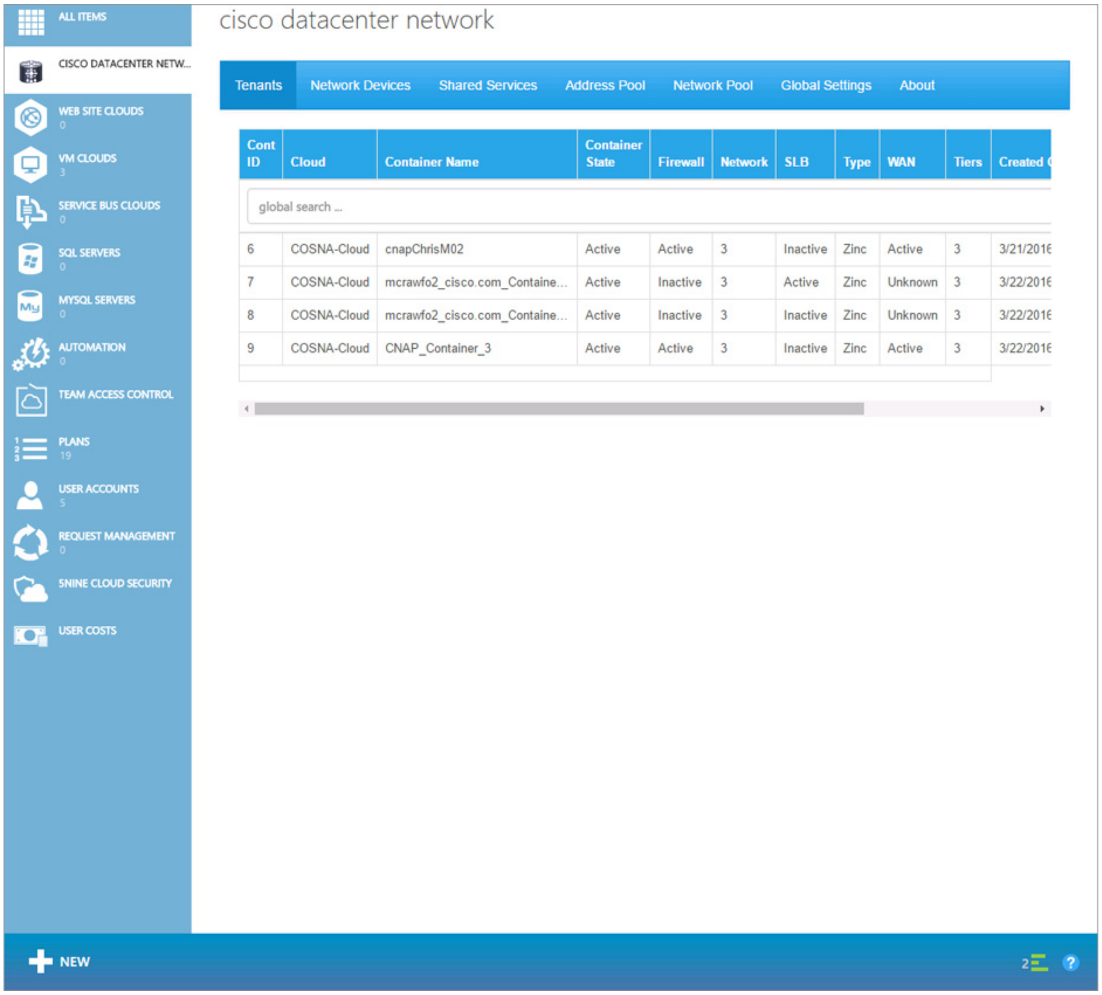
Step 1 Access WAP as an administrator.

For information on accessing WAP, see the WAP documentation.

Step 2 In the WAP interface, in the left column, click **Cisco Datacenter Network**.

You see the main Cisco Datacenter Network screen, which is the Tenants tab, as shown in the following screen.

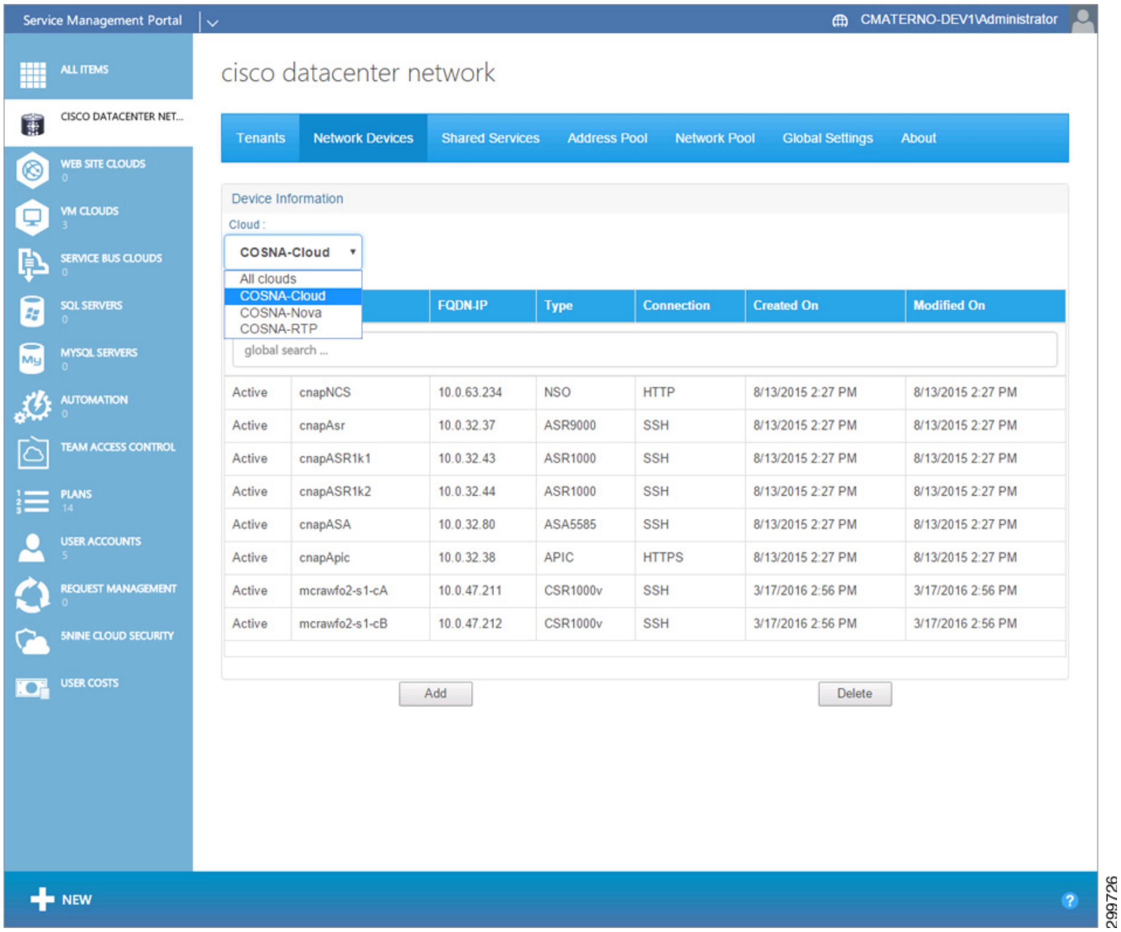
Figure 1-35 Tenants Tab Screen



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created (
6	COSNA-Cloud	cnapChrisM02	Active	Active	3	Inactive	Zinc	Active	3	3/21/2016
7	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Active	Zinc	Unknown	3	3/22/2016
8	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/22/2016
9	COSNA-Cloud	CNAP_Container_3	Active	Active	3	Inactive	Zinc	Active	3	3/22/2016

Step 3 Click **Network Devices** and on the Network Devices Tab screen, in the Cloud drop-down, click the cloud service to which you want to add a device, as shown in the following screen.

Figure 1-36 Network Devices Tab Screen



cisco datacenter network

Device Information

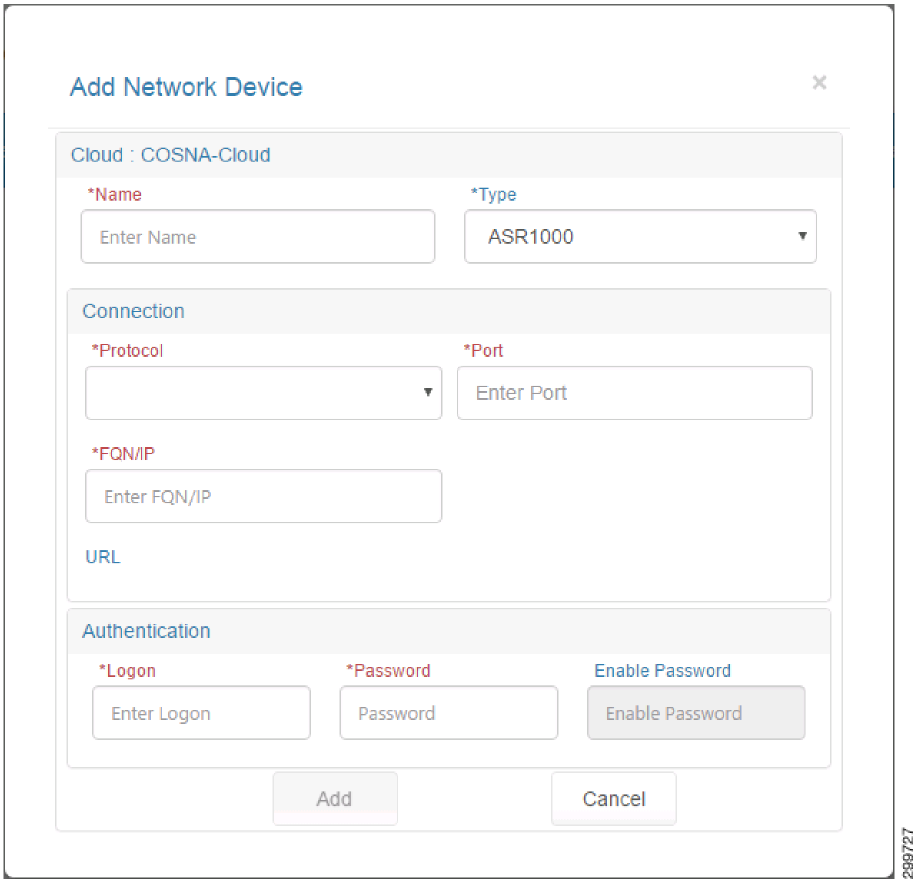
Cloud : COSNA-Cloud

		FQDN-IP	Type	Connection	Created On	Modified On
Active	cnapNCS	10.0.63.234	NSO	HTTP	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapAsr	10.0.32.37	ASR9000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASR1k1	10.0.32.43	ASR1000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASR1k2	10.0.32.44	ASR1000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASA	10.0.32.80	ASA5585	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapApic	10.0.32.38	APIC	HTTPS	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	mcrawfo2-s1-cA	10.0.47.211	CSR1000v	SSH	3/17/2016 2:56 PM	3/17/2016 2:56 PM
Active	mcrawfo2-s1-cB	10.0.47.212	CSR1000v	SSH	3/17/2016 2:56 PM	3/17/2016 2:56 PM

Step 4 Click **Add**.

You see the Add Network Device screen.

Figure 1-37 Add Network Device Screen



Add Network Device

Cloud : COSNA-Cloud

*Type: ASR1000

Step 5 Cloud: *Cloud Name* displays the Cloud Service to which the Cisco NSO will be associated. Complete the following fields:

- Name—User-defined name given to the Network Device.
- Type—Device type: On the pull-down menu, select **NSO**.
- Connection:
  - Protocol—Protocol used to connect to the device: SSH, HTTP, or HTTPS.
  - Port—Port used to establish the connection to the device.
  - FQDN/IP—Valid IP Address in dotted format or Fully Qualified Name (FQN) given to the Network Device at the Provider's Network. Characters, numbers, and "-". (The period [.] is also used in DNS names, but only between DNS labels and at the end of an FQDN.) https://technet.microsoft.com/en-us/library/cc959336.aspx
- Authentication:
  - Login—Service Account Logon used to establish a connection with the Network Device.
  - Password—Service account password. The entry field on the dialog **must** be set to show a "*" for each character entered for password.
  - Enable Password—If the Cisco NSO you are adding has an enable password that is different than the device password, enter it here. Otherwise the device password will be used for enable mode.

Step 6 Click **Add** to add the Cisco NSO or **Cancel** to cancel the addition.

Connecting Cisco Cloud Network Automation Provisioner to Managed Devices

In addition to connecting Cisco CNAP to Cisco NSO, you must also add other devices in the Admin Portal, such as the Cisco ASR9000, Cisco APIC, etc.

For more information, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 1.1*.

Post-Installation Verification Overview

The following table summarizes the verification process for the various components.

Component	Verification Point
Cisco CNAP Admin	Web App CiscoNetworkAdmin exists under <*drive*>:\inetpub\MgmtSvc-AdminSite\Content at the Microsoft WAP Admin Management Portal Host. Login to the Admin Portal. Verify that the Cisco CNAP RP appears in Microsoft WAP's Available Resources. Create a "Test Plan" and verify creation success
Cisco CNAP Tenant	Web App CiscoNetworkTenant exists under <*drive*>:\inetpub\MgmtSvc-TenantSite\Content at the Microsoft WAP Tenant Management Portal Host. Login to the Tenant Portal. Create a Subscription to "Test Plan", verify that "Test Plan" is selectable for subscription, and verify creation success. Verify that the subscription is created. Configure the subscription with default container settings, monitor container creation, and verify creation success.

Cisco CNAP API and Provisioner	Cisco CNAP RP API MgmtSvc-CiscoNetwork exists under <*drive*>:\inetpub at the Microsoft WAP Admin API Host. Web Service MgmtSvc-CiscoNetwork can be started and stopped in Microsoft IIS Manager. Cisco CNAP Provisioner MgmtSvc-CiscoNetwork exists under <*drive*>:\Program Files\Management Service\Cisco at the WAP Admin API Host. Windows Service Cisco.Network.Provisioner is listed in Service Management with Status = Empty (Not Running), Startup Type= Automatic, and Logon Account = Account provided during installation. Microsoft Service Provider Foundation is reachable from the Microsoft WAP Admin API Host.
Cisco CNAP Database	Database CCA_DB exists at the SLQ server provided during installation (Microsoft WAP SQL Management DB Server).
Cisco Network Service Orchestrator (NSO)	Cisco Network Services Orchestrator Enabled by Tail-f successfully deployed on the Management Hyper-V Cluster. Cisco Network Services Orchestrator Enabled by Tail-f can successfully access the Infrastructure through the Management Network.

Using Cisco Cloud Network Automation Provisioner

You access the Admin Portal and Tenant Portal from the WAP interface.

Accessing the Admin Portal

To access the Admin Portal:

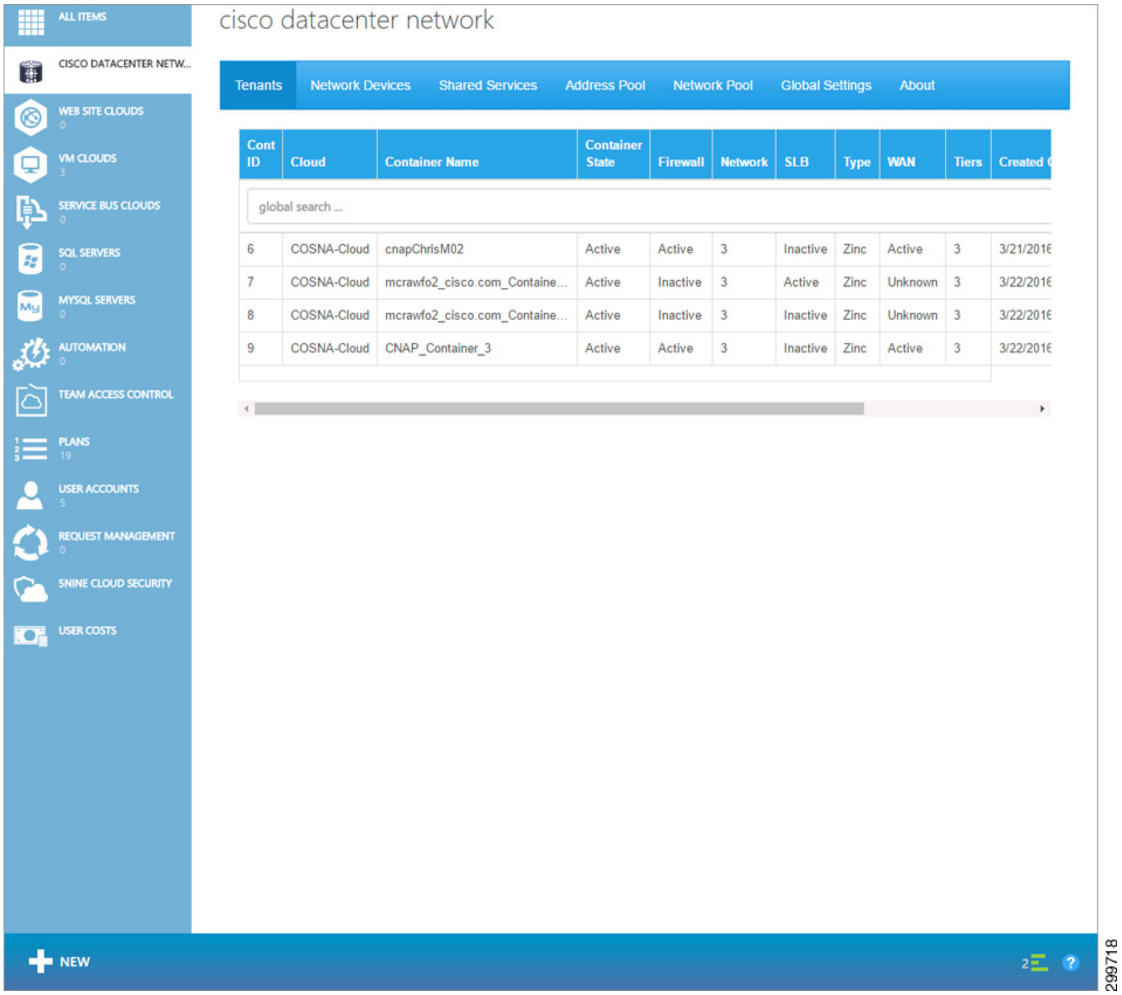
Step 1 Access the WAP Admin Site and log in as an administrator.

For information on accessing WAP, see the WAP documentation.

Step 2 In the WAP Admin Site, in the left column, click **Cisco Datacenter Network**.

You see the main Cisco Datacenter Network screen, which is the Tenants tab, as shown in the following screen.

Figure 1-38 Tenants Tab Screen



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created (
6	COSNA-Cloud	cnapChrisM02	Active	Active	3	Inactive	Zinc	Active	3	3/21/2016
7	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Active	Zinc	Unknown	3	3/22/2016
8	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/22/2016
9	COSNA-Cloud	CNAP_Container_3	Active	Active	3	Inactive	Zinc	Active	3	3/22/2016

For more information, see:

- *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 1.1*

Accessing the Tenant Portal

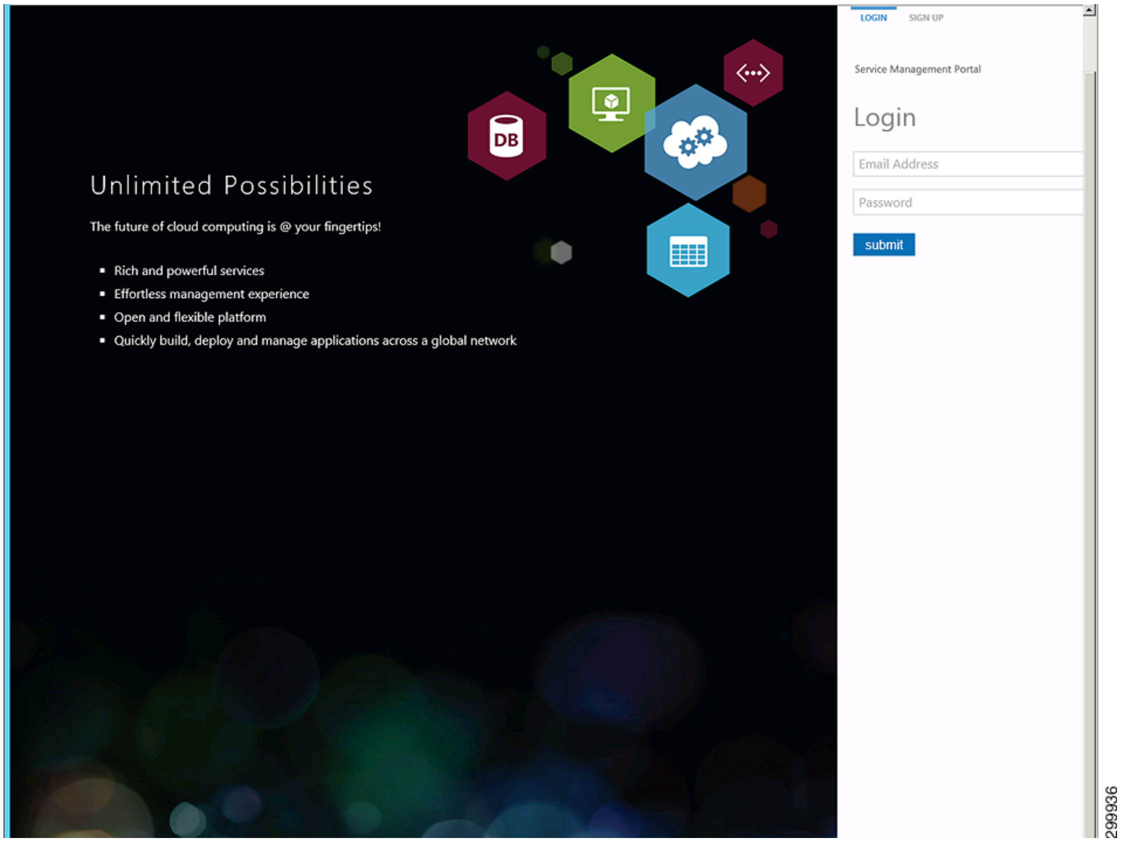
To access the Tenant Portal:

Step 1 Access the WAP Tenant Site.

For information on accessing WAP, see the WAP documentation.

You see the WAP Tenant Portal Login screen, as shown in the following screen.

Figure 1-39 WAP Tenant Portal Login Screen



Unlimited Possibilities

The future of cloud computing is @ your fingertips!

- Rich and powerful services
- Effortless management experience
- Open and flexible platform
- Quickly build, deploy and manage applications across a global network

Service Management Portal

Login

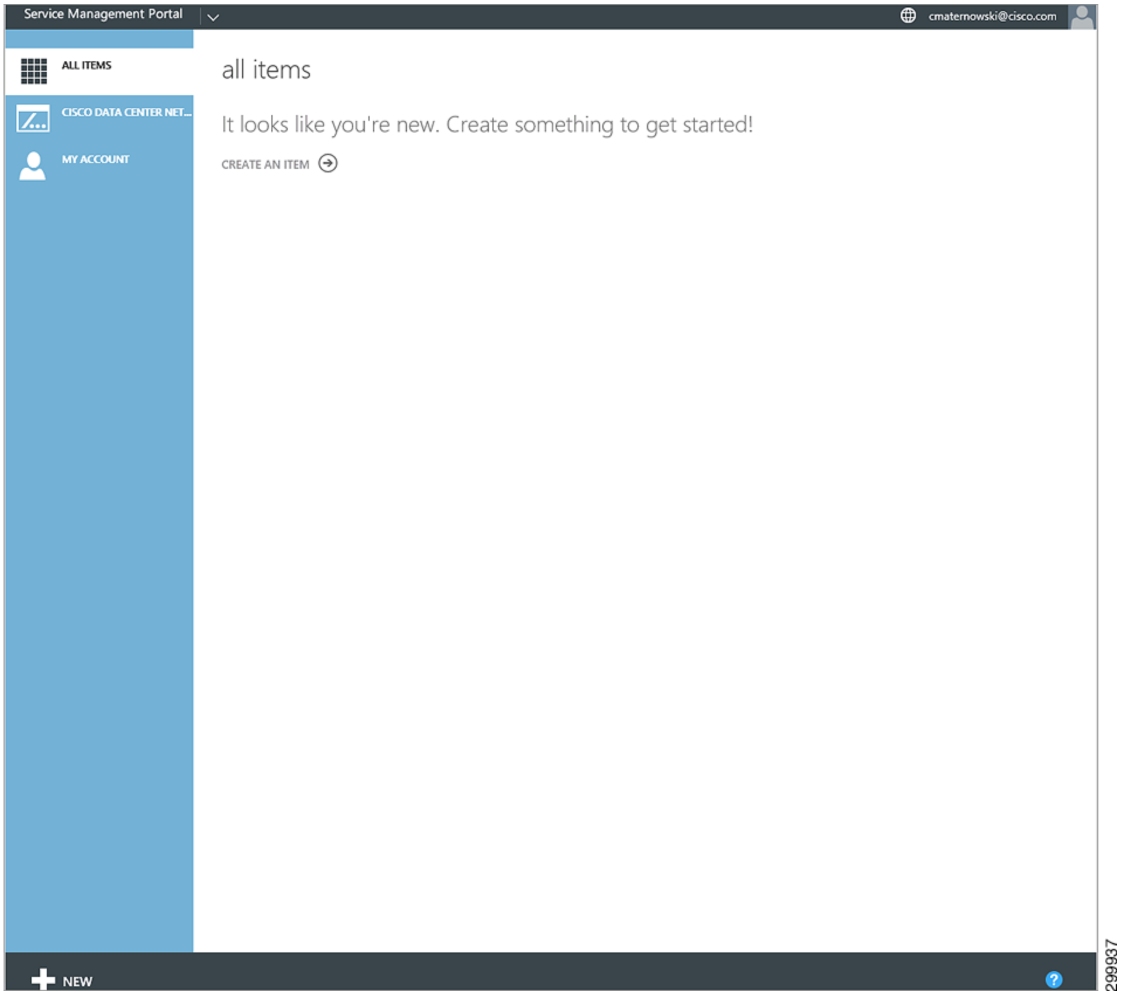
Email Address

Password

Step 2 Enter your login credentials, then click **submit**.

You see the Tenant Portal main screen, as shown in the following screen.

Figure 1-40 Tenant Portal Main Screen



Service Management Portal

cmaternowski@cisco.com

all items

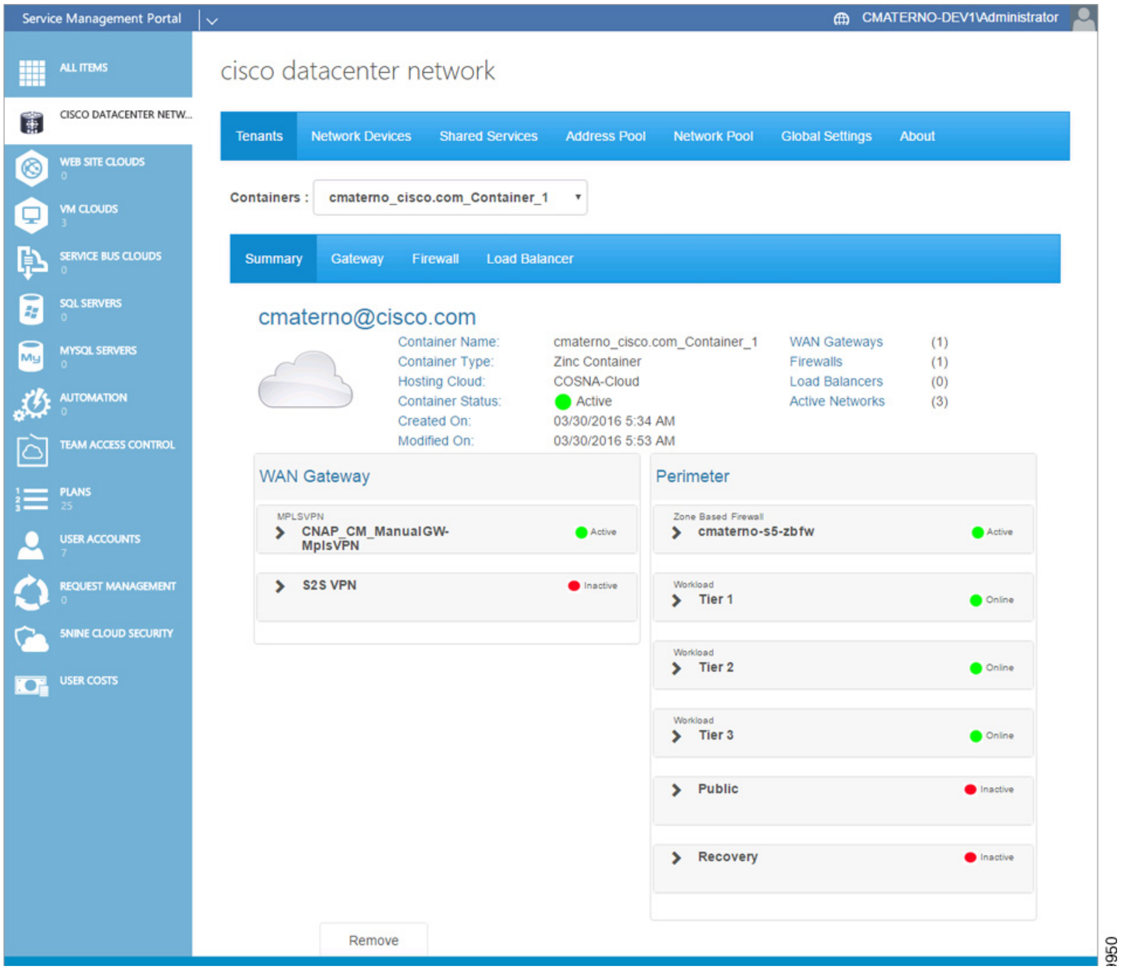
It looks like you're new. Create something to get started!

CREATE AN ITEM

Step 3 In the WAP interface, in the left column, click **Cisco Datacenter Network**.

You see the main Cisco Datacenter Center screen, as shown in the following screen.

Figure 1-41 Tenant Portal Cisco Datacenter Network Screen



Containers : cmaterno_cisco.com_Container_1

cmaterno@cisco.com

Container Name:	cmaterno_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(0)
Container Status:	● Active	Active Networks	(3)
Created On:	03/30/2016 5:34 AM		
Modified On:	03/30/2016 5:53 AM		

WAN Gateway

- MPLSVPN — CNAP_CM_ManualGW-MplsVPN — ● Active
- S2S VPN — ● Inactive

Perimeter

- Zone Based Firewall — cmaterno-s5-zbfw — ● Active
- Workload — Tier 1 — ● Online
- Workload — Tier 2 — ● Online
- Workload — Tier 3 — ● Online
- Public — ● Inactive
- Recovery — ● Inactive

For more information, see:

- *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1*

Appendix A—Using a Script to Install Cisco Cloud Network Automation Provisioner

You can use the VBScript script packaged with Cisco CNAP to install it. The advantage of using a script is that you can specify various parameters, such as run in quiet mode, produce logs that can be useful in debugging installation issues, etc.

Running this script first removes all previous installations of the Cisco CNAP and then installs the specified instance.

Run the script, which is named setup.vbx, via the administrator command line to quickly install Cisco CNAP with predefined values you specify.

The arguments to the script are as follows (all values are case sensitive):

- /feature:{**backend**/**admin**/**tenant**/**all**}—Select the feature(s) you want to install. There is no default. If you do not specify a /feature argument, then the script runs the standard installer and launches the GUI with no options selected, but with logging enabled.
- /quiet:{**true**/**false**}—Choose to run the installer silently or not. If the installer runs silently, you do not see any installer GUI screen. The default is false.
- /iniFile:<*path to .ini file*>—Specify an .ini file that contains values for the various parameters required to install the backend service (the install script currently only supports specifying values for the backend service feature). There is no default value. See Installing the Admin Site for the various values that have to be specified. The format of the .ini file should follow that of the example ini file provided with the installer package.

Appendix B—Troubleshooting Installation Issues

Accessing Logs and Identifying Issues

Installation logs are not produced when using the GUI to install Cisco CNAP. However you can use a script packaged with Cisco CNAP to install it; the script. produces logs that can be useful in debugging installation issues. For more information, see Appendix A—Using a Script to Install Cisco Cloud Network Automation Provisioner.

Contacting Customer Support

For Cisco customer support, see:

- Cisco Support and Downloads
  http://www.cisco.com/c/en/us/support/index.html

Troubleshooting Microsoft Windows Azure Pack

For information on troubleshooting Microsoft WAP, see:

- Windows Azure Pack troubleshooting
  https://technet.microsoft.com/en-us/library/dn554311.aspx

Also see the list of references in the section Useful Microsoft Windows Azure Pack References.